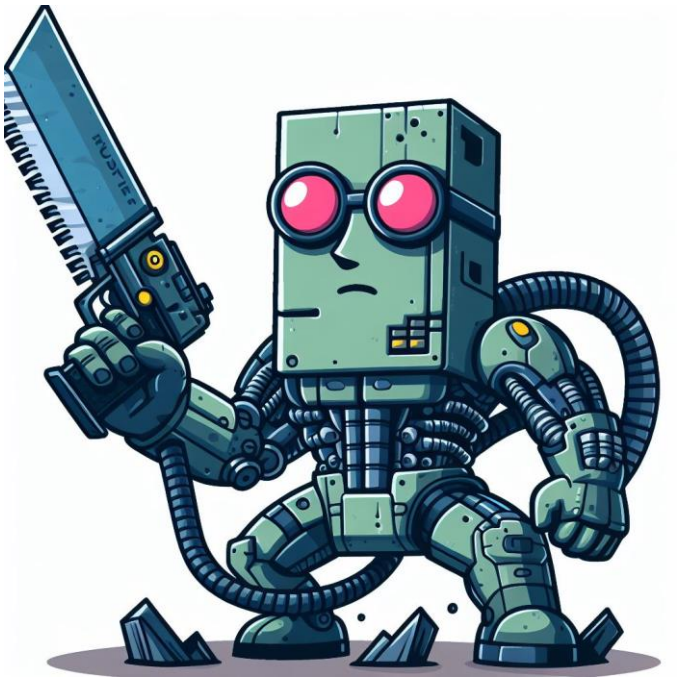

Аннотация – В этом документе представлен анализ вредоносного ПО "Infamous Chisel", приписываемого группе Sandworm. В анализе рассматриваются различные аспекты вредоносного ПО, включая его возможности, компоненты и последствия его развёртывания против конкретных целей, в частности устройств Android.

Анализируя компоненты и тактику вредоносного ПО, документ проливает свет на сложную природу киберугроз и их потенциал для компрометации конфиденциальной информации и нарушения операций. Выводы подчёркивают острую необходимость в упреждающих мерах защиты.

Для специалистов по кибербезопасности и других направлений этот анализ служит ценным ресурсом для понимания механизма и последствий продвинутых вредоносных угроз. Материалы документа могут послужить основой для разработки более эффективных стратегий и технологий защиты, повышения уровня безопасности организаций ввиду постоянно меняющегося ландшафта киберугроз.

I. Введение

Вредоносная программа Chisel нацелена на устройства Android, обеспечивая удалённый доступ и кражу информации с этих устройств. Sandworm использовал это вредоносное ПО в кампании, направленной против устройств Android, используемых в военном секторе. Вредоносное ПО представляет собой набор компонентов, которые обеспечивают постоянный доступ к заражённому устройству Android через сеть Tor, а также периодически сопоставляют и извлекают информацию о жертве со скомпрометированных устройств. Украденная информация включает в себя информацию о системных устройствах, информацию о коммерческих приложениях и приложениях, специфичных для военного сектора.

II. Компоненты печально известного долота

Infamous Chisel — это набор компонентов, связанных с Sandworm, предназначенных для обеспечения удалённого доступа и сбора информации с телефонов Android.

В состав Infamous Chisel входят:

- **netd:** компонент используется для автоматического сбора и фильтрации информации об устройстве. Он также ищет в нескольких каталогах файлы, соответствующие заранее определённому набору расширений, которые затем удаляются.
- **killer**: компонент убивает процесс netd.
- **blob**: компонент выполняется netd и отвечает за настройку и выполнение утилиты Tor td.
- **td**: утилита представляет собой Tor без очевидных модификаций.
- **tcpdump**: утилита представляет собой tcpdump без очевидных модификаций.
- **ndbr_armv7l и ndbr_i686:** эти утилиты содержат: dropbear, dropbearkey, ssh, scp, nmap, dbclient, watchdog, rmflag, mkflag.
- **db:** утилита содержит: dropbear, dropbearkey, ssh, scp, nmap, dbclient, watchdog, rmflag, mkflag.

III. Сетевые и другие возможности

Infamous Chisel предназначен для закрепления в системе путём замены штатного системного двоичного файла netd по пути /system/bin/netd. Когда вредоносный netd запускается, он проверяет, является ли init родительским процессом, который его выполнил. Этот родительский процесс отвечает за создание процессов, перечисленных в скрипте init.rc. Вредоносная замена netd при таком выполнении разветвится и выполнит штатный процесс, резервную копию которого зарезервировали по пути /system/bin/netd_, передав параметры командной строки. Это сохраняет нормальную функциональность netd, в то же время позволяя вредоносному netd выполняться от имени пользователя root.

Компонент netd предоставляет большую часть пользовательских функций. Основная его цель — сбор и извлечение информации со скомпрометированного устройства через определённые промежутки времени. Он использует комбинацию сценариев оболочки и команд для сбора информации об устройстве и также выполняет поиск в нескольких каталогах, в которые попадают файлы согласно определённому набору критериев.

Infamous Chisel имеет несколько других возможностей:

- **Мониторинг сети и сбор трафика:** может отслеживать сетевую активность и собирать данные о сетевом трафике. Это позволяет собирать информацию о сетевой среде и перехватывать конфиденциальные данные, передаваемые по сети.

- **Доступ по SSH:** может устанавливать соединения SSH, которые можно использовать для удалённого выполнения команд и передачи данных.
- **Сканирование сети.** может сканировать локальную сеть, собирая информацию об активных хостах, открытых портах и баннерах для идентификации другие потенциальные цели в сети.
- **Передача файлов SCP:** может использовать протокол безопасного копирования (SCP) для передачи файлов. Это может быть использовано для кражи данных с заражённого устройства или для переноса вредоносных файлов на устройство.
- **Эксфильтрация информации:** выполняет периодическое сканирование файлов и сетевой информации на предмет кражи. Файлы конфигурации системы и приложений удалены с заражённого устройства.
- **Сбор информации об устройствах:** собирает различную информацию о системных устройствах, информацию о коммерческих приложениях и приложениях, специфичных для военного сектора.
- **Автоматическая эксфильтрация:** удаляет файлы через определённые промежутки времени.
- **Остановка службы:** может остановить штатную службу netd.

IV. Эксплуатируемые уязвимости

Chisel использует различные уязвимости и методы для обеспечения несанкционированного доступа и контроля над целевыми устройствами Android, например комбинацию уязвимостей системы, небезопасных конфигураций и сетевых протоколов для достижения своих целей. К ним относятся закрепление и повышенных привилегий, предотвращения обнаружения, доступ к учётным данным, сбор конфиденциальной информации, создание скрытых каналов управления и контроля и потенциальное перемещение внутри сети. Основные уязвимости и методы включают (без конкретного CVE):

- **Закрепление и повышение привилегий:** закрепление обеспечивается на заражённом устройстве путём замены штатного системного двоичного файла netd. Эта замена позволяет вредоносному netd выполняться от имени пользователя root, тем самым получая повышенные привилегии.
- **Предотвращение обнаружения.** использует несколько методов предотвращение обнаружения. Например, проверяется, выполняется ли Chisel с помощью init и по пути к штатного netd, что снижает вероятность обнаружения его вредоносных действий. Кроме того, компонент blob распаковывает исполняемые файлы из архивов bzip, что может быть способом избежать обнаружения путём распаковки его полезных данных только после того, как они прошли первоначальные проверки безопасности.
- **Доступ к учётным данным:** используется утилиту tcpdump для анализа сетевых интерфейсов и мониторинга сетевого трафика, потенциально перехватывая учётные данные, передаваемые по сети. Он также извлекается информация из определённых файлов, содержащих учётные данные и ключевую информацию с использованием системным механизмов доступа.
- **Обнаружение и сбор:** выполняются действия по обнаружению и сбору, такие как перебор каталогов данных для обнаружения интересующих файлов, сбор информации GPS, составление списка установленных пакетов и сбор различной системной информации. Это указывает на то, что Chisel использует отсутствие применения безопасного хранилища и неправильные настройки разрешений на устройстве для доступа и сбора конфиденциальной информации.
- **C2C и эксфильтрация:** настраивает и запускает Tor со скрытым сервисом Dropbear для обеспечения SSH-соединения. Такая настройка позволяет вредоносному ПО установить скрытый канал связи с заражённым устройством, используя сетевые протоколы и службы для сохранения контроля над устройством и кражи собранных данных.
- **Сетевое сканирование и распространение.** содержит функции сканирования локальной сети, сбора информации об активных хостах, открытых портах и баннерах. Эта возможность предполагает, что Chisel использует сетевое окружение заражённого устройства для выявления других потенциальных целей в сети для горизонтального перемещения или дальнейшего использования.

V. Эксфильтрация данных

Chisel собирает информацию с заражённых Android-устройств посредством ряда автоматических и ручных процессов. Вредоносное ПО, связанное с субъектом угрозы Sandworm, выполняет периодическое сканирование файлов и сетевой информации на предмет кражи. Он ищет файлы, соответствующие заранее определённому набору параметров, и удаляет файлы конфигурации системы и приложений с заражённого устройства. Подробно процесс эксфильтрации выглядит следующим образом:

- **Хеширование файлов и предотвращение дублирования.** Когда файл выбран для эксфильтрации, он хешируется с использованием MD5 и перекрёстно ссылается на список ранее отправленных хэшей файлов, хранящихся в файле в одном из трех мест, поддерживающих разные версии Android. Это гарантирует, что один и тот же файл не будет отправлен несколько раз.
- **Эксфильтрация файлов из каталогов данных**. программа ищет в указанных каталогах файлы с определёнными расширениями и удаляет их.

- **Эксфильтрация файлов конфигурации и резервных копий конфигурации**. Вредоносная программа ищет файлы.json или.json.bak в указанных каталогах и удаляет их.
- **Эксфильтрация файлов.** программа удаляет файлы с помощью POST-запроса. Ожидается, что ответ сервера будет HTTP, и эксфильтрация считается завершённой, когда сервер отправляет сообщение «Успех» в любом месте своего ответа.
- **Сбор и фильтрация информации:** собирает различную информацию о конфигурации оборудования устройства и записывает эту информацию в файлы в каталоге /data/local, которые затем удаляются. Сюда входит идентификатор Android, сетевая информация, список установленных приложений и различная информация об оборудовании устройства.
- **Сканирование локальной сети.** включает в себя встроенный сетевой сканер, который выполняет сканирование IP-адресов локальной сети для обнаружения других устройств. Результаты этого сканирования немедленно передаются, предоставляя злоумышленникам информацию, которая может облегчить горизонтальное перемещение внутри сети.
- **Частота эксфильтрации.** ПО предназначено для автоматического удаления файлов через регулярные промежутки времени, при этом определённые интервалы устанавливаются для различных типов сбора данных. Например, сбор информации о файлах и устройствах происходит каждые 23 часа 53 минуты, а конфиденциальная информация перекачивается каждые 10 минут.
- **Использование Tor и SSH для безопасной эксфильтрации:** Chisel использует Tor и SSH для C2C-связи, обеспечивая зашифрованный канал, который может быть трудно обнаружить и перехватить. Такая настройка позволяет ПО поддерживать скрытый канал связи с заражённым устройством, что усложняет обнаружение и устранение последствий.

Когда файл выбирается для эксфильтрации, он хешируется по MD5 и перекрёстно ссылается на список ранее отправленных хэшей файлов, хранящихся в файле в одном из трёх мест, поддерживающих разные версии Android. Будет использоваться первый существующий путь к каталогу: /sdcard/Android/data/.google.index, /storage/emulated/0/Android/data/.google.index или storage/emulated/1/Android/data/.google.index.

Эксфильтрация файла считается завершённой, когда сервер отправляет сообщение «Успех» в любом месте своего ответа. Для этой эксфильтрации используется POST протокола передачи гипертекста (HTTP), и ожидается, что ответ сервера также будет HTTP, но это явно не проверяется. 16 необработанных байтов MD5 добавляются в конец файла.google.index, гарантируя, что один и тот же файл не будет отправлен несколько раз. Поскольку файл.google.index содержит необработанные байты, без предварительного уведомления может показаться, что он содержит случайные данные. Начальный размер составляет 256 КБ, заполненный значениями NULL, что обеспечивает пространство для максимум 16 384 хэшей файлов. Все записи хеша будут проверены для каждого файла перед эксфильтрацией. Когда достигается конец файла.google.index, позиция сбрасывается на начало, перезаписывая предыдущие хэши. Это означает, что, если количество файлов, подлежащих удалению с устройства, превысит 16 384, файлы будут отправлены несколько раз.

Компонент netd запускает таймеры о выполнение различных задач, включая утечку информации о файлах и устройствах. Этот процесс происходит каждые 86 000 секунд (приблизительно 23 часа, 53 минуты и 20 секунд), в течение которых вредоносная программа ищет в указанных каталогах файлы, соответствующие списку расширений, и собирает различную информацию о конфигурации оборудования устройства. Собранная информация хранится в каталоге /data/local, а затем удаляется.

VI. Влияние и географический охват

Влияние Infamous Chisel на устройства Android значительно и приводит к потере конфиденциальной информации, нарушению конфиденциальности и потенциальному использованию устройства для дальнейших вредоносных действий.

Chisel в первую очередь нацелен на устройства Android, используемые военным сектором. Кампания была выявлена когда о ней сообщили несколько организаций, в том числе Национальный центр кибербезопасности Великобритании (NCSC), Агентство национальной безопасности США (NSA), Агентство по кибербезопасности и инфраструктурной безопасности США (CISA), Федеральное бюро расследований США (ФБР), Национальный центр кибербезопасности Новой Зеландии (NCSC-NZ)., Канадский центр кибербезопасности и Австралийское управление связи (ASD).

VII. Пути заражения

Основываясь на возможностях и методах работы, описанных в документе, можно сделать вывод о некоторых потенциальных векторах заражения, которые использует столь сложная вредоносная кампания:

- **Фишинговые атаки.** могут использоваться методы фишинга, чтобы обманом заставить пользователей установить вредоносные приложения или перейти по ссылкам, ведущим к загрузке вредоносного ПО.
- **Использование уязвимостей.** Могут использоваться известные уязвимости в операционной системе Android или установленных приложениях для получения несанкционированного доступа и установки.
- **Социальная инженерия.** социальная инженерия используется, чтобы убедить пользователей предоставить разрешения или отключить функции

безопасности, которые в противном случае помешали бы выполнению или закреплению вредоносного ПО.

- **Сторонние магазины приложений:** Chisel может распространяться через сторонние магазины приложений или веб-сайты, предлагающие заражённые версии оригинальных приложений.
- **Вредоносная реклама.** Вредоносная реклама может перенаправлять пользователей на веб-сайты, которые автоматически загружают и устанавливают вредоносное ПО на их устройства.
- **Целевой фишинг.** кампании целевого фишинга могут использоваться для заражения устройств конкретных лиц или организаций вредоносным ПО.
- **Chain-атаки.** взлом цепочек поставок программного обеспечения с целью внедрения вредоносного кода в легитимные приложения.

VIII. Проактивные и реактивные меры

Подход к защите от таких сложных кампаний вредоносного ПО обычно включает в себя сочетание превентивных и реактивных мер кибербезопасности. Кроме того, получение информации о последних киберугрозах и сотрудничество с агентствами по кибербезопасности и отраслевыми партнёрами могут повысить способность организации защищаться от таких угроз.

Проактивные меры включают в себя:

- **Осведомлённость и обучение кибербезопасности**: обучение сотрудников рискам вредоносного ПО и важности соблюдения передовых методов обеспечения безопасности, таких как отказ от перехода по подозрительным ссылкам или загрузки непроверенных вложений.
- **Регулярные обновления программного обеспечения**: обеспечение актуальности всего ПО, включая ОС и приложения, с использованием новейших исправлений безопасности для устранения известных уязвимостей.
- **Надёжные антивирусные и антивирусные решения:** развёртывание комплексных антивирусных и вредоносных решений, которые могут обнаруживать и предотвращать выполнение вредоносного кода на устройствах организации.
- **Сетевая безопасность:** реализация мер сетевой безопасности, таких как брандмауэры, системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS), для мониторинга и контроля входящего и исходящего сетевого трафика на основе применённого набора правил.
- **Контроль доступа:** обеспечение строгого контроля доступа и использование принципа наименьших привилегий, чтобы гарантировать, что пользователи имеют только доступ, необходимый для выполнения их рабочих функций.
- **Планирование реагирования на инциденты:** разработка и поддержание плана реагирования на инциденты для быстрого и эффективного реагирования на потенциальные инциденты безопасности.

Реактивные меры включают в себя:

- **Обмен информацией об угрозах:** участие в обмене информацией об угрозах с другими организациями и агентствами по кибербезопасности, чтобы быть в курсе последних угроз и стратегий их устранения.
- **Мониторинг и обнаружение:** постоянный мониторинг систем на предмет признаков компрометации и наличие механизмов обнаружения для оповещения о подозрительных действиях.
- **Криминалистический анализ:** проведение криминалистического анализа в случае нарушения безопасности для понимания масштабов компрометации, устранения угрозы и восстановления затронутых систем.
- **Регулярные проверки безопасности:** проведение регулярных проверок безопасности и оценок уязвимостей для выявления и устранения пробелов в безопасности в инфраструктуре организации.
- **Резервное копирование и восстановление:** регулярное резервное копирование важных данных и наличие плана аварийного восстановления для восстановления операций в случае атаки вредоносного ПО.

Меры для устройств Android:

- **Регулярное обновление:** следует регулярно обновлять ОС Android и все установленные приложения, чтобы гарантировать устранение известных уязвимостей. Вредоносное ПО часто использует недостатки безопасности в устаревшем программном обеспечении.
- **Установка программное обеспечение безопасности.** Применение надёжных антивирусных решений, разработанных для устройств Android. Они могут помочь обнаружить и удалить вредоносное программное обеспечение.
- **Неизвестные источники:** необходимо отключить установку приложений из неизвестных источников в настройках устройства и использовать доверенные магазины приложений (например, Google Play Store).
- **Осторожность при работе со ссылками и вложениями.** Не следует переходить по ссылкам и загружать вложения из неизвестных или подозрительных источников. Фишинг —

распространённый метод распространения вредоносного ПО.

- **Применение VPN.** При подключении к общедоступным сетям Wi-Fi следует использовать VP) для шифрования интернет-соединения и защиты от перехвата сети.
- **Применение двухфакторной аутентификации (2FA).** Использование 2FA для сетевых учётных записей добавит дополнительный уровень безопасности, что усложнит злоумышленникам доступ, даже если им удастся украсть учётные данные.
- **Мониторинг сетевого трафика.** Для организаций мониторинг сетевого трафика на предмет необычной активности может помочь обнаружить наличие вредоносных программ, таких как Infamous Chisel. Внедрение сегментации сети, чтобы ограничить распространение вредоносного ПО.
- **Резервное копирование важных данных:** следует регулярно выполнять резервирование важных данных, хранящихся на устройстве. В случае заражения вредоносным ПО наличие резервных копий может предотвратить потерю данных.
- **Шифрование устройства:** использование шифрования устройства для защиты данных на устройстве. Это затрудняет злоумышленникам доступ к информации, если устройство взломано.
- **Ограничение разрешений приложений:** необходимо регулярно проверять и ограничивать разрешения, предоставленные приложениям. Ограничение разрешений может уменьшить объем данных, к которым может получить доступ приложение, тем самым ограничивая то, что может быть украдено вредоносным ПО.