BI.ZONE

THREAT ZONE 2025: ОБРАТНАЯ СТОРОНА

Исследование теневых ресурсов

Оглавление

Введение

Современные кибератаки, управляемые человеком, часто основаны на принципах разделения и кооперации труда. При взломе компаний злоумышленники используют не только собственные самописные программы, но и коммерческое вредоносное ПО (ВПО) — стилеры, крипторы, загрузчики, трояны удаленного доступа и другое. Кроме того, предметом купли-продажи становятся эксплоиты к уязвимостям, базы данных, первоначальные доступы ко взломанным сетям и услуги, связанные с проведением атак. Все это формирует полноценную теневую экосистему, где программные инструменты, данные и услуги распространяются по рыночным законам.

Теневые ресурсы, на которых продаются перечисленные товары и услуги, — это зеркало намерений атакующих. Именно здесь появляются сигналы будущих атак: обсуждаются конкретные цели, формируются ценовые ориентиры и складываются тренды. Без учета этой информации ландшафт киберугроз остается неполным. Таким образом, нелегальные форумы, телеграм-каналы и чаты становятся важным звеном в современной цепочке кибератак.

Наиболее популярные площадки для продажи товаров и услуг — классические даркнет-форумы, разнообразные каналы и чаты в Telegram, Discord и других мессенджерах, а также маркетплейсы с автоматизированной системой продаж. Каждая из этих площадок имеет свою структуру и правила взаимодействия.

Изучение объявлений на этих ресурсах дает информацию о взломанных компаниях, типах продаваемых доступов, актуальном ВПО и инструментах, которые будут использоваться в реальных атаках. Кроме того, такие объявления содержат технические детали, позволяющие идентифицировать тактики и техники из MITRE ATT&CK. Эти же детали помогают косвенно оценивать масштаб и направленность киберпреступной активности в отношении определенных стран и отраслей.

Для этого исследования мы проанализировали содержимое десятков теневых форумов и тысяч сообщений в телеграм-каналах, чтобы выявить риски, которые оно представляет для компаний в России и СНГ. В поле нашего внимания попали ВПО, эксплоиты, доступы к корпоративным сетям, а также услуги, связанные с кибератаками.

При этом мы стремились извлечь из данных практическую пользу. Нашей задачей было показать, что из текста объявлений можно выявлять прямые признаки конкретных техник из матрицы MITRE ATT&CK. Эти данные позволяют не только изучать общие тренды, но и оперативно сопоставлять полученную информацию с текущими средствами защиты в инфраструктуре компаний. Такой подход помогает оценить, насколько инфраструктура устойчива к техникам, которые открыто обсуждаются на теневых площадках и уже применяются в атаках.

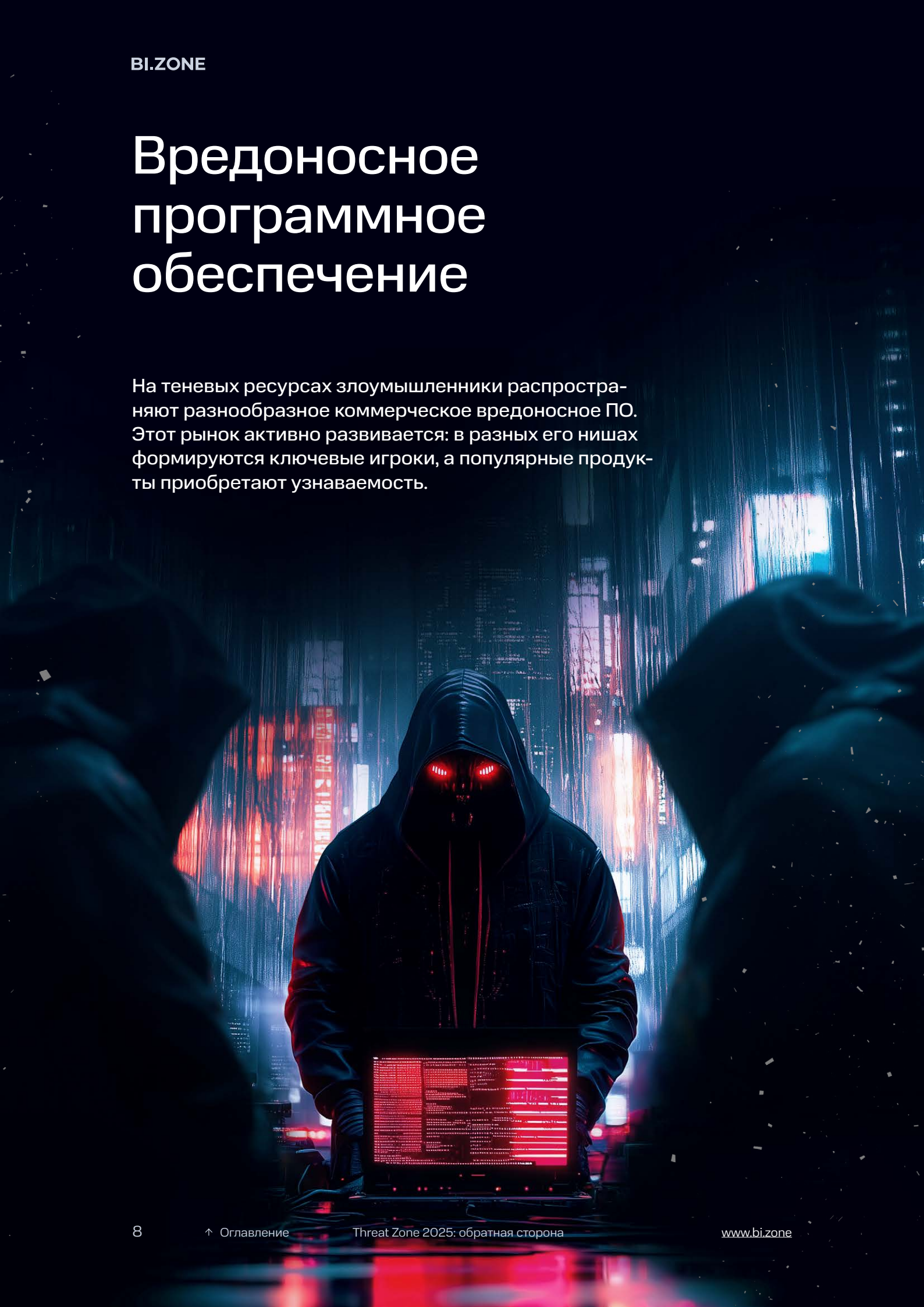
В основу исследования «Threat Zone 2025: обратная сторона» легли результаты анализа более чем 5000 сообщений, которые были размещены злоумышленниками на теневых ресурсах в 2024-м и первой половине 2025 года.

Исследование носит исключительно технически прикладной характер. Его ключевая задача — продемонстрировать, как данные, полученные по результатам анализа теневых ресурсов, позволяют предсказывать кибератаки. В частности, такая информация помогает выявлять уязвимости, инструменты, а также тактики, техники и процедуры до того, как злоумышленники начали применять их для реализации кибератак.

Информация, представленная в исследовании, предназначена для специалистов в области кибербезопасности, руководителей и владельцев компаний, а также всех организаций, заинтересованных в выстраивании комплексной киберзащиты.

Вредоносное программное обеспечение

На теневых ресурсах злоумышленники распространяют разнообразное коммерческое вредоносное ПО. Этот рынок активно развивается: в разных его нишах формируются ключевые игроки, а популярные продукты приобретают узнаваемость.

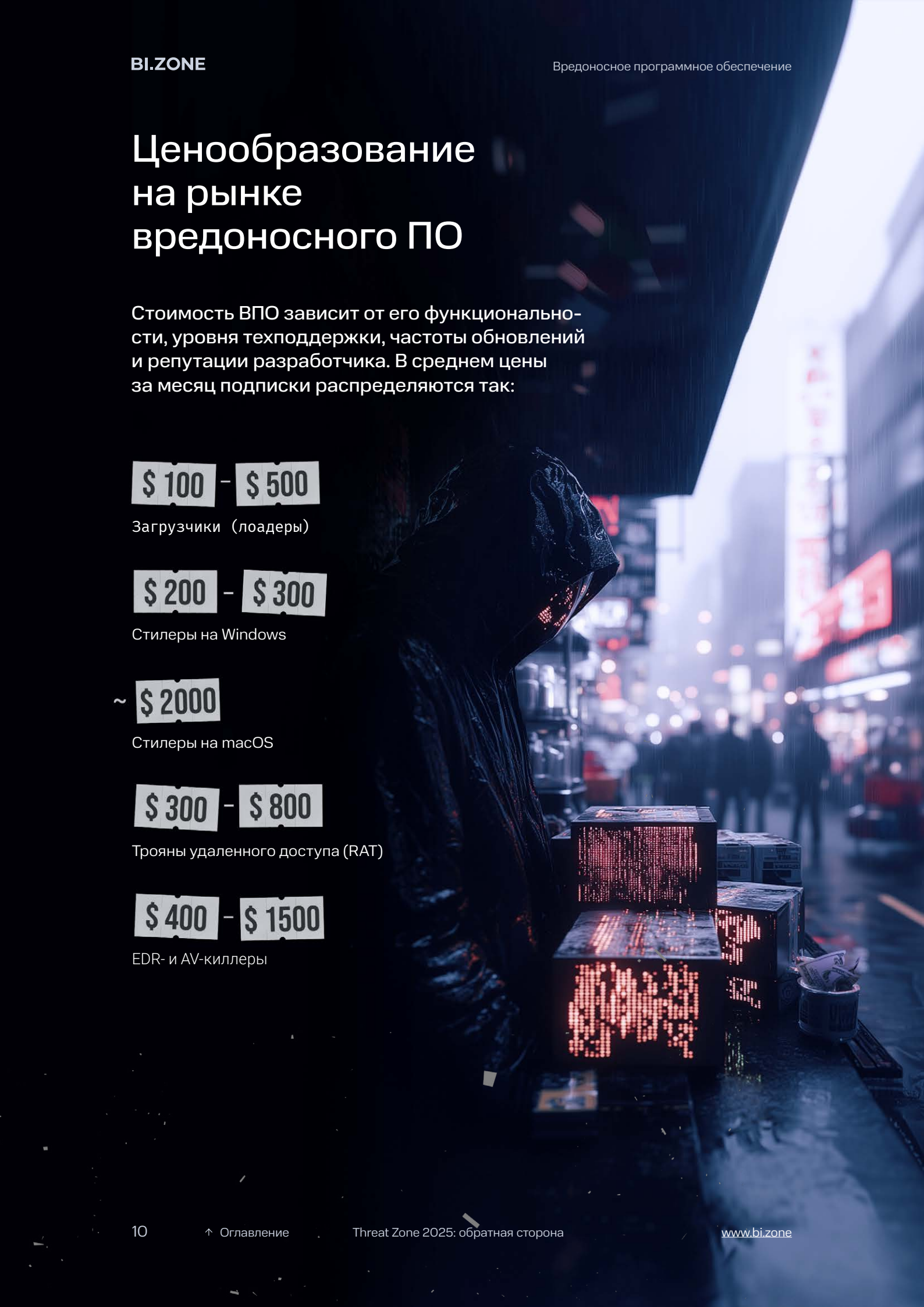


Взаимодействие продавцов и покупателей строится в основном по модели malware-as-a-service (вредоносное ПО как услуга, MaaS). В этом случае разработчики предлагают свои продукты по подписке, сопровождая их инструкциями и регулярными обновлениями. Такой подход значительно снижает порог входа для киберпреступников, позволяя проводить атаки даже тем, кто не обладает глубокими техническими знаниями.

Некоторые из рассмотренных нами инструментов уже давно используются в кампаниях на территории России и стран СНГ. Среди жертв — самые разные организации: корпорации и средний бизнес, коммерческие компании и госучреждения.

Ценообразование на рынке вредоносного ПО

Стоимость ВПО зависит от его функциональности, уровня техподдержки, частоты обновлений и репутации разработчика. В среднем цены за месяц подписки распределяются так:



Особняком стоят программы-вымогатели. На международном рынке они обычно распространяются по модели ransomware-as-a-service (программа-вымогатель как услуга, RaaS): разработчик получает процент от выкупа — как правило, 10–40%. Стоимость ВПО определяется не только функциональностью, но и известностью «бренда», а также условиями партнерской программы. Как правило, она предполагает процент с выкупа (обычно 20–40%) и единоразовый взнос за доступ к платформе (1000–3000 $).
О том, как устроен российский рынок RaaS и чем отличается от зарубежного, мы поговорим в рамках раздела о программах-вымогателях.

Как устроена первая часть исследования

В ней мы анализируем объявления о продаже вредоносного ПО. На конкретных примерах показываем, насколько ценную информацию может дать изучение сообщений на теневых форумах и в телеграм-каналах. Благодаря им делаем выводы о ключевых характеристиках и наиболее востребованных типах ВПО.

Всего рассматриваем пять категорий инструментов:

- загрузчики,
- стилеры,
- RAT,
- EDR- и AV-киллеры,
- программы-вымогатели.

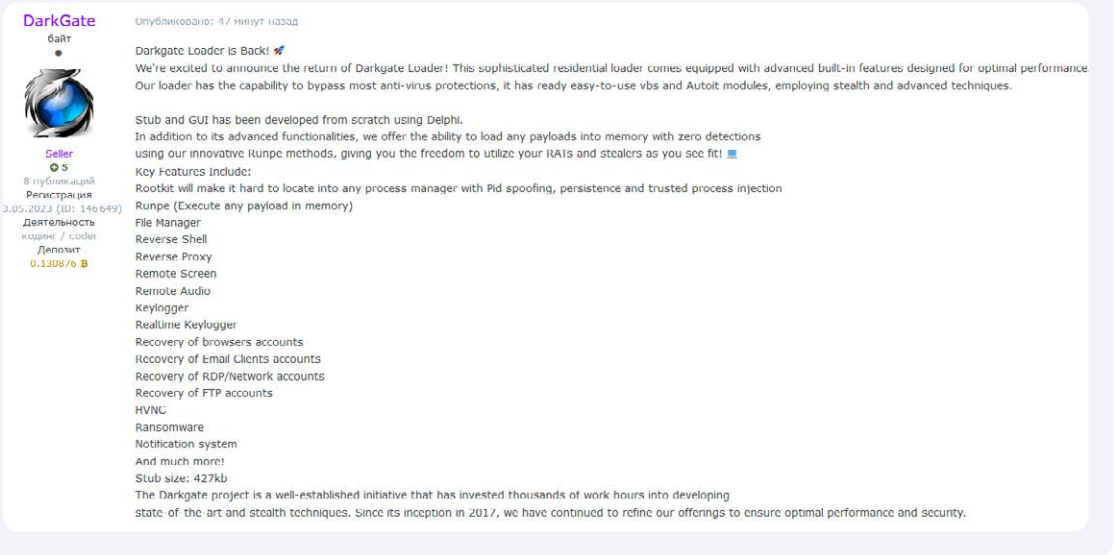
Там, где это применимо, мы сопоставляем полученные данные об инструменте с техниками, описанными в MITRE ATT&CK.

Загрузчики

DarkGate Loader

DarkGate — вредоносное ПО, написанное с нуля на Delphi, распространяется через теневые форумы с 2017 года. Разработчик позиционирует его в качестве высокофункционального и сложнодетектируемого инструмента для доставки вредоносной нагрузки, включая RAT, стилеры и программы-вымогатели.

Объявление о продаже загрузчика DarkGate на теневом форуме



DarkGate
байт

Seller
5
8 публикаций
Регистрация
3.05.2023 (ID: 146 649)
Деятельность
кодинг / coder
Депозит
0.1308/6 ฿

Опубликовано: 47 минут назад

Darkgate Loader is Back! 🚀
We're excited to announce the return of Darkgate Loader! This sophisticated residential loader comes equipped with advanced built-in features designed for optimal performance
Our loader has the capability to bypass most anti-virus protections, it has ready easy-to-use vbs and Autoit modules, employing stealth and advanced techniques.

Stub and GUI has been developed from scratch using Delphi.
In addition to its advanced functionalities, we offer the ability to load any payloads into memory with zero detections
using our innovative Runpe methods, giving you the freedom to utilize your RATs and stealers as you see fit! 💻
Key Features include:
Rootkit will make it hard to locate into any process manager with Pid spoofing, persistence and trusted process injection
Runpe (Execute any payload in memory)
File Manager
Reverse Shell
Reverse Proxy
Remote Screen
Remote Audio
Keylogger
Realtime Keylogger
Recovery of browsers accounts
Recovery of Email Clients accounts
Recovery of RDP/Network accounts
Recovery of FTP accounts
HVNC
Ransomware
Notification system
And much more!
Stub size: 427kb
The Darkgate project is a well-established initiative that has invested thousands of work hours into developing
state of the art and stealth techniques. Since its inception in 2017, we have continued to refine our offerings to ensure optimal performance and security.

Основной акцент в описании ВПО делается на способности незаметно загружать программы, необходимые для проведения атаки. Для скрытной загрузки инструмент использует Visual Basic Script (VBS), AutoIt-скрипты и другие продвинутые техники.

Однако возможности загрузчика не ограничиваются лишь загрузкой. В его функциональность также входят:

- инструменты удаленного доступа;
- кейлоггер;
- скрытая запись экрана;
- извлечение учетных данных из браузеров, почтовых клиентов, FTP-программ;
- шифровальщик данных;
- система отправки уведомлений и другие возможности.

Широкая функциональность и относительно высокая стоимость указывают на то, что загрузчик не предназначен для массовых кампаний. Скорее он ориентирован на длительное скрытное присутствие в скомпрометированной сети и может использоваться не только для первоначальной доставки ВПО, но и на этапе постэксплуатации.

Статью с подробным анализом DarkGate читайте на нашем сайте.

MITRE ATT&CK

Тактика	Техника	Процедура
Execution	Command and Scripting Interpreter	DarkGate использует модуль реверс-шелла, выполняющий удаленные команды в интерпретаторе команд ОС
	Command and Scripting Interpreter: Visual Basic	DarkGate может выполнять сценарии VBS
	Command and Scripting Interpreter: AutoHotKey & AutoIT	DarkGate может выполнять сценарии AutoIt
Persistence	Boot or Logon Autostart Execution	DarkGate закрепляется в автозагрузке системы
Privilege Escalation	Access Token Manipulation: Parent PID Spoofing	DarkGate использует техники спуффинга идентификатора родительского процесса (PPID)

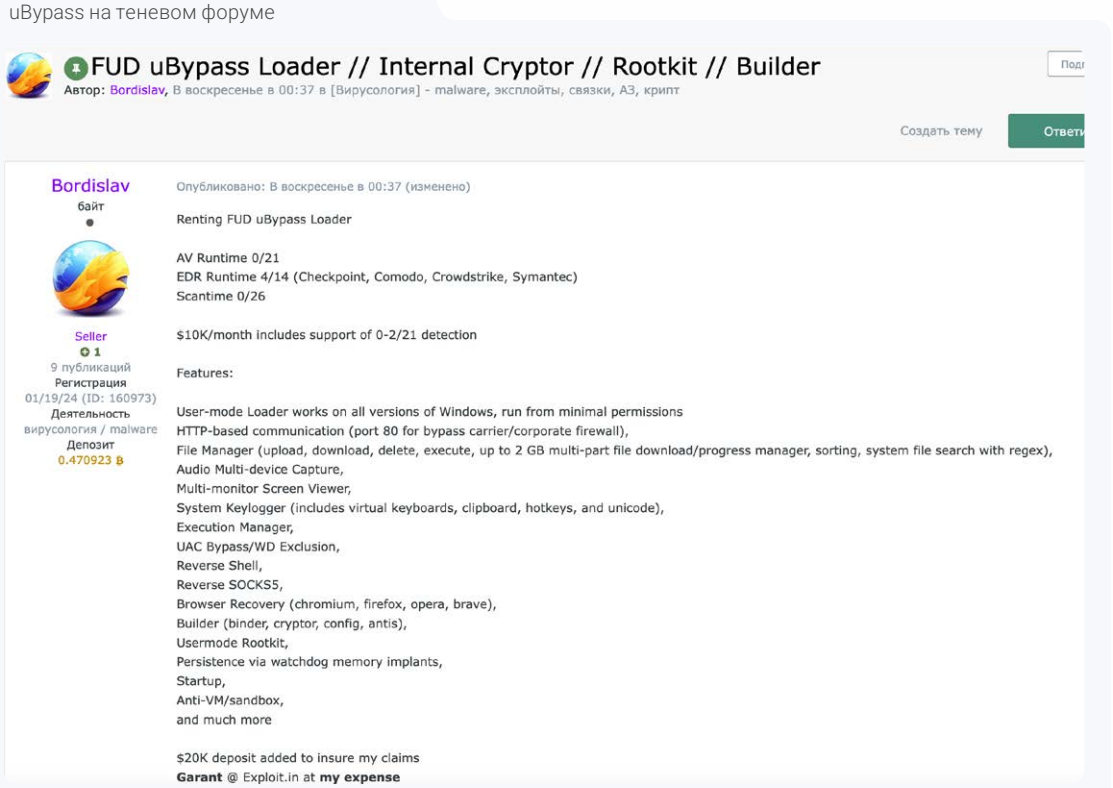
Тактика	Техника	Процедура
Defense Evasion	Obfuscated Files or Information	DarkGate обходит большинство антивирусных защит, предположительно за счет обфускации
	Process Injection	DarkGate использует различные техники Runpe для внедрения кода в доверенные процессы и выполнения нагрузки в памяти целевого процесса
	Rootkit	DarkGate использует модуль руткита
Credential Access	Credentials from Password Stores	DarkGate извлекает данные учетных записей браузеров, почтовых клиентов, RDP, FTP
Lateral Movement	Remote Services	DarkGate использует модуль HVNC (Hidden Virtual Network Computing)
Collection	Audio Capture	DarkGate способен записывать звук аудиоустройств
	Input Capture: Keylogging	DarkGate использует модуль кейлоггера
	Screen Capture	DarkGate способен создавать снимки экрана рабочего стола
Command and Control	Proxy	DarkGate использует модуль обратного прокси (реверс-прокси)
Impact	Data Encrypted for Impact	DarkGate использует модуль шифрования данных

DarkGate уже задокументирован в MITRE ATT&CK.
Ознакомьтесь с подробной матрицей по ссылке.

uBypass Loader

uBypass Loader — еще один загрузчик с широкими функциональными возможностями. Автор утверждает, что за 10 000 $ в месяц в рамках технической поддержки гарантируется минимальный уровень детектируемости ВПО. Кроме того, в объявлении подчеркивается, что загрузчик позволяет обойти в том числе ряд EDR-решений и лишь несколько могут его обнаружить.

Объявление о продаже загрузчика uBypass на теневом форуме



Коммуникация с C2-сервером происходит через порт 80, что позволяет таким соединениям смешаться с легитимным трафиком. Загрузчик помогает обойти UAC (User Account Control) и добавляет экземпляр в исключения Windows Defender, а также ограничивает собственное выполнение в виртуальных средах.

Помимо функций загрузчика, uBypass Loader выполняет и другие. Например, позволяет:

- работать с файлами в скомпрометированной системе,
- записывать аудио,
- получать доступ к экрану,
- извлекать сохраненные данные из браузеров,
- использовать реверс-шелл и реверс-прокси.

Также загрузчик реализует функции кейлоггера и руткита.

Инструмент отличается высокой стоимостью, но за счет широкой функциональности позволяет злоумышленникам совершать целевые, управляемые человеком атаки даже на организации с высоким уровнем кибербезопасности.

MITRE ATT&CK

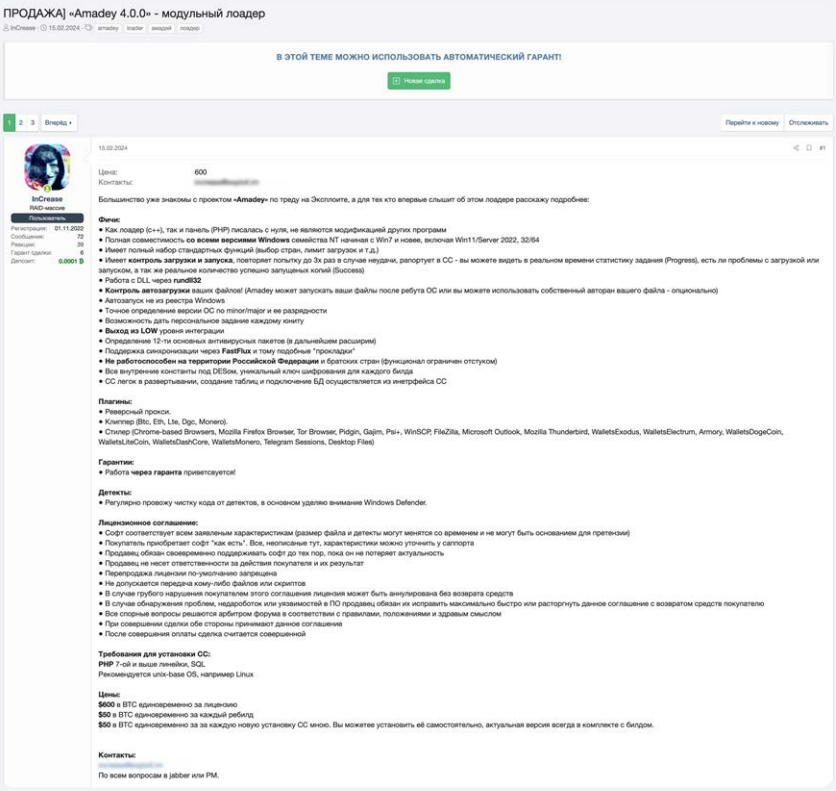
Тактика	Техника	Процедура
Execution	Command and Scripting Interpreter	uBypass Loader использует модуль реверс-шелла, выполняющий удаленные команды в интерпретаторе команд ОС
Persistence	Boot or Logon Autostart Execution	uBypass Loader закрепляется в автозагрузке системы
Defense Evasion	Impair Defenses: Disable or Modify Tools	uBypass Loader обходит UAC (User Account Control) и добавляет себя в исключения Windows Defender
	Obfuscated Files or Information	uBypass Loader поддерживает шифрование в моменте сборки (билдер)
	Process Injection	uBypass Loader способен внедрять watchdog-импланты в память процессов
	Rootkit	uBypass Loader использует руткит в пользовательском режиме (usermode)
	Virtualization/Sandbox Evasion	uBypass Loader затрудняет анализ в виртуальных машинах и песочницах
Credential Access	Credentials from Password Stores	uBypass Loader извлекает данные учетных записей браузеров (Chromium, Firefox, Opera, Brave), а также RDP

Тактика	Техника	Процедура
Collection	Archive Collected Data	uBypass Loader поддерживает загрузку файлов и папок с хоста на сервер в виде ZIP-архивов
	Audio Capture	uBypass Loader способен записывать звук аудиоустройств
	Input Capture: Keylogging	uBypass Loader использует системный кейлоггер
	Screen Capture	uBypass Loader способен создавать снимки экрана рабочего стола
Command and Control	Application Layer Protocol: Web Protocols	uBypass Loader использует сетевой порт 80 (HTTP) для обхода межсетевых экранов
	Ingress Tool Transfer	uBypass Loader загружает в скомпрометированную систему другие вредоносные программы
	Non-Application Layer Protocol	uBypass Loader использует протокол SOCKS5 в обратном прокси
	Proxy	uBypass Loader использует обратный SOCKS5-прокси

Amadey

Amadey — еще один пример загрузчика, который не ограничивается базовыми функциями, а также расширяет возможности за счет плагинов.

Объявление о продаже загрузчика Amadey на теневом форуме



ПРОДАЖА] «Amadey 4.0.0» - модульный лоадер

В ЭТОЙ ТЕМЕ МОЖНО ИСПОЛЬЗОВАТЬ АВТОМАТИЧЕСКИЙ ГАРАНТ!

Новая сделка

Перейти к новому | Отслеживать

InCrease
RAID-массив
Пользователь

Цена: 600
Контакты:

Большинство уже знакомы с проектом **«Amadey»** по треду на Эксплоите, а для тех кто впервые слышит об этом лоадере расскажу подробнее:

Фичи:
• Как лоадер (c++), так и панель (PHP) писалась с нуля, не являются модификацией других программ
• Полная совместимость **со всеми версиями Windows** семейства NT начиная с Win7 и новее, включая Win11/Server 2022, 32/64
• Имеет полный набор стандартных функций (выбор стран, лимит загрузок и т.д.)
• Имеет **контроль загрузки и запуска**, повторяет попытку до 3х раз в случае неудачи, рапортует в CC - вы можете видеть в реальном времени статистику задания (Progress), есть ли проблемы с загрузкой или запуском, а так же реальное количество успешно запущеных копий (Success)
• Работа с DLL через **rundll32**
• **Контроль автозагрузки** ваших файлов! (Amadey может запускать ваши файлы после ребута ОС или вы можете использовать собственный авторан вашего файла - опционально)
• Автозапуск не из реестра Windows
• Точное определение версии ОС по minor/major и ее разрядности
• Возможность дать персональное задание каждому юниту
• **Выход из LOW** уровня интеграции
• Определение 12-ти основных антивирусных пакетов (в дальнейшем расширим)
• Поддержка синхронизации через **FastFlux** и тому подобные "прокладки"
• **Не работоспособен на территории Российской Федерации** и братских стран (функционал ограничен отстуком)
• Все внутренние константы под DESом, уникальный ключ шифрования для каждого билда
• CC легок в развертывании, создание таблиц и подключение БД осуществляется из инетрфейса CC

Плагины:
• Реверсный прокси.
• Клиппер (Btc, Eth, Ltc, Dgc, Monero).
• Стилер (Chrome-based Browsers, Mozilla Firefox Browser, Tor Browser, Pidgin, Gajim, Psi+, WinSCP, FileZilla, Microsoft Outlook, Mozilla Thunderbird, WalletsExodus, WalletsElectrum, Armory, WalletsDogeCoin, WalletsLiteCoin, WalletsDashCore, WalletsMonero, Telegram Sessions, Desktop Files)

Гарантии:
• Работа **через гаранта** приветсвуется!

Детекты:
• Регулярно провожу чистку кода от детектов, в основном уделяю внимание Windows Defender.

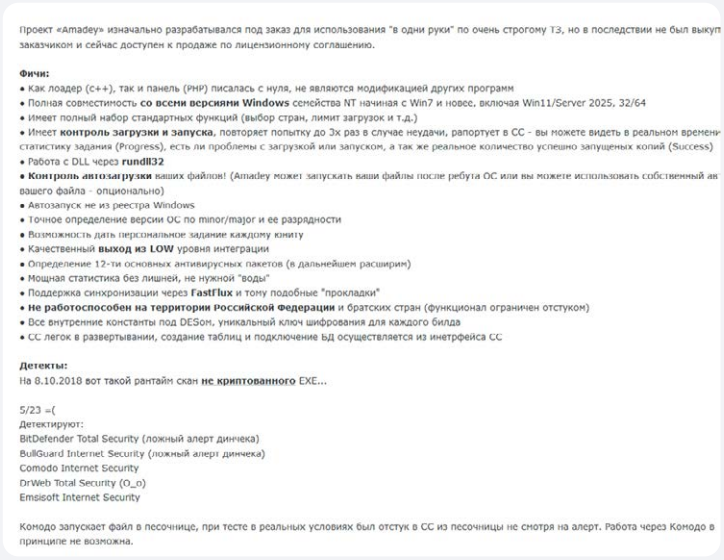
Лицензионное соглашение:
• Софт соответствует всем заявленым характеристикам (размер файла и детекты могут менятся со временем и не могут быть основанием для претензий)
• Покупатель приобретает софт "как есть". Все, неописаные тут, характеристики можно уточнить у саппорта
• Продавец обязан своевременно поддерживать софт до тех пор, пока он не потеряет актуальность
• Продавец не несет ответственности за действия покупателя и их результат
• Перепродажа лицензии по-умолчанию запрещена
• Не допускается передача кому-либо файлов или скриптов
• В случае грубого нарушение покупателем этого соглашения лицензия может быть аннулирована без возврата средств
• В случае обнаружения проблем, недоработок или уязвимостей в ПО продавец обязан их исправить максимально быстро или расторгнуть данное соглашение с возвратом средств покупателю
• Все спорные вопросы решаются арбитром форума в соответствии с правилами, положениями и здравым смыслом
• При совершении сделки обе стороны принимают данное соглашение
• После совершения оплаты сделка считается совершеной

Требования для установки CC:
PHP 7-ой и выше линейки, SQL
Рекомендуется unix-base OS, например Linux

Цены:
$600 в BTC единовременно за лицензию
$50 в BTC единовременно за каждый ребилд
$50 в BTC единовременно за за каждую новую установку CC мною. Вы можете установить её самостоятельно, актуальная версия всегда в комплекте с билдом.

Контакты:
По всем вопросам в jabber или PM.

Описание загрузчика Amadey на теневом форуме



Проект «Amadey» изначально разрабатывался под заказ для использования "в одни руки" по очень строгому ТЗ, но в последствии не был выкуп заказчиком и сейчас доступен к продаже по лицензионному соглашению.

Фичи:
• Как лоадер (c++), так и панель (PHP) писалась с нуля, не являются модификацией других программ
• Полная совместимость **со всеми версиями Windows** семейства NT начиная с Win7 и новее, включая Win11/Server 2025, 32/64
• Имеет полный набор стандартных функций (выбор стран, лимит загрузок и т.д.)
• Имеет **контроль загрузки и запуска**, повторяет попытку до 3х раз в случае неудачи, рапортует в CC - вы можете видеть в реальном времени статистику задания (Progress), есть ли проблемы с загрузкой или запуском, а так же реальное количество успешно запущеных копий (Success)
• Работа с DLL через **rundll32**
• **Контроль автозагрузки** ваших файлов! (Amadey может запускать ваши файлы после ребута ОС или вы можете использовать собственный ав вашего файла - опционально)
• Автозапуск не из реестра Windows
• Точное определение версии ОС по minor/major и ее разрядности
• Возможность дать персональное задание каждому юниту
• Качественный **выход из LOW** уровня интеграции
• Определение 12-ти основных антивирусных пакетов (в дальнейшем расширим)
• Мощная статистика без лишней, не нужной "воды"
• Поддержка синхронизации через **FastFlux** и тому подобные "прокладки"
• **Не работоспособен на территории Российской Федерации** и братских стран (функционал ограничен отстуком)
• Все внутренние константы под DESом, уникальный ключ шифрования для каждого билда
• CC легок в развертывании, создание таблиц и подключение БД осуществляется из инетрфейса CC

Детекты:
На 8.10.2018 вот такой рантайм скан **не криптованного** EXE...

5/23 =(
Детектируют:
BitDefender Total Security (ложный алерт динчека)
BullGuard Internet Security (ложный алерт динчека)
Comodo Internet Security
DrWeb Total Security (O_o)
Emsisoft Internet Security

Комодо запускает файл в песочнице, при тесте в реальных условиях был отстук в CC из песочницы не смотря на алерт. Работа через Комодо в принципе не возможна.

Автор подчеркивает, что ВПО не использует системный реестр для закрепления в скомпрометированной системе, а также поддерживает формат DLL и запуск через rundll32. Amadey позволяет получить базовую информацию о скомпрометированной системе, а также информацию об установленном антивирусном ПО. Для коммуникаций с C2-сервером может использоваться fast flux DNS.

Также автор предлагает плагины для загрузчика. Они, в частности, позволяют:

- использовать реверс-прокси;
- извлекать сохраненные учетные данные из браузеров и других приложений;
- подменять строки в буфере обмена, похожие на адреса криптокошельков.

В объявлении подчеркивается, что загрузчик нельзя применять в атаках на территории России и некоторых других стран. Стоимость лицензии составляет 600 $, при этом за дополнительную плату можно заказать разные услуги, например настройку командного сервера.

MITRE ATT&CK

Тактика	Техника	Процедура
Persistence	Boot or Logon Autostart Execution	Amadey закрепляется в автозагрузке системы
Defense Evasion	Obfuscated Files or Information	Amadey использует алгоритм DES
	System Binary Proxy Execution: Rundll32	Amadey запускает DLL через rundll32
Credential Access	Credentials from Password Stores	Amadey позволяет извлечь учетные данные из различных браузеров, мессенджеров, почтовых клиентов, FTP-клиентов

Тактика	Техника	Процедура
Discovery	Software Discovery: Security Software Discovery	Amadey проверяет наличие установленных антивирусных средств в системе
	System Information Discovery	Amadey определяет версию и разрядность ОС
	System Location Discovery	Amadey определяет географическое расположение жертвы с целью предотвратить запуск на территории России и стран СНГ
Collection	Clipboard Data	Amadey использует плагин-клиппер для модификации данных в буфере обмена
	Data from Local System	Amadey собирает данные в скомпрометированной системе и отправляет их на командный сервер
Command and Control	Dynamic Resolution: Fast Flux DNS	Amadey использует Fast Flux DNS для взаимодействия с командными серверами
	Proxy	Amadey может использовать реверс-прокси

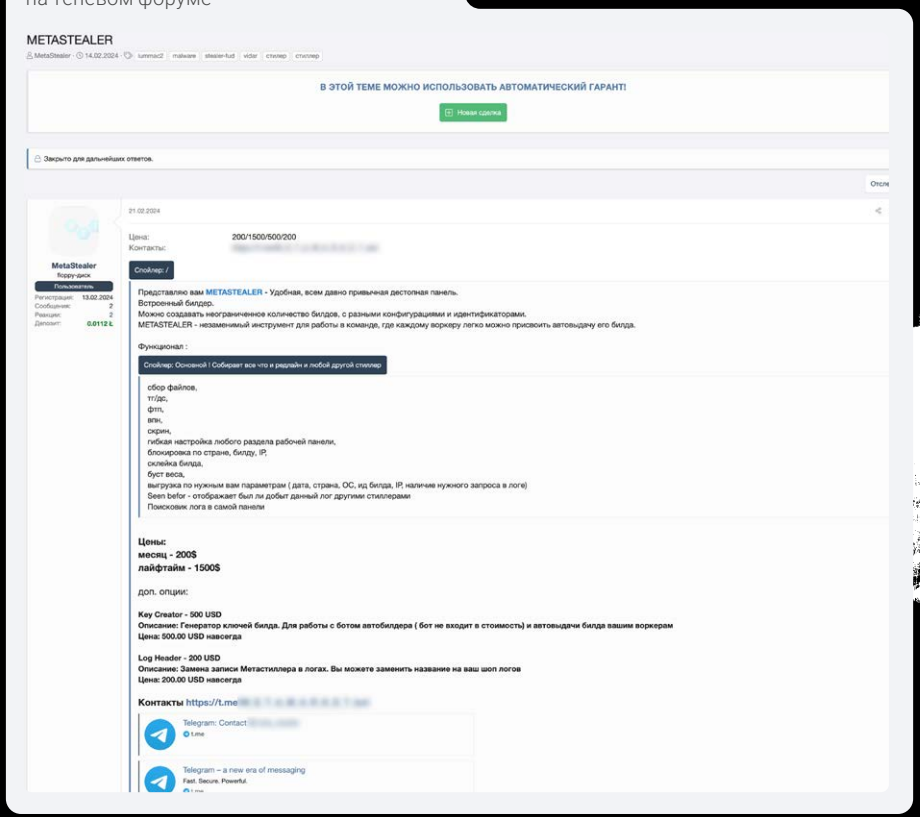
Amadey уже задокументирован в MITRE ATT&CK. Ознакомьтесь с подробной матрицей по ссылке.

Стилеры

MetaStealer

MetaStealer распространяется через теневые форумы и Telegram. В основе лежит модифицированный исходный код стилера RedLine, из которого были удалены ограничения на использование в России и странах СНГ.

Объявление о продаже MetaStealer на теневом форуме



Разработчик позиционирует его как удобный, современный и гибко настраиваемый стилер с панелью администрирования.

ВПО работает с Windows и специализируется на сборе конфиденциальных данных:

- извлекает учетные данные из браузеров на движках Chromium и Gecko (включая пароли, сохраненные в расширениях);
- собирает данные из криптовалютных кошельков, системные данные и файлы определенных форматов.

Помимо этого, продавец предлагает и уникальные функции. Например, проверку наличия собранных данных среди уже имеющихся, а также автоматический поиск фраз для восстановления криптокошельков. Также доступен криптор, а в будущем продавец обещает добавить и загрузчик.

Группировка Venture Wolf активно использовала MetaStealer в атаках на российские компании. Узнайте подробности в статье.

MITRE ATT&CK

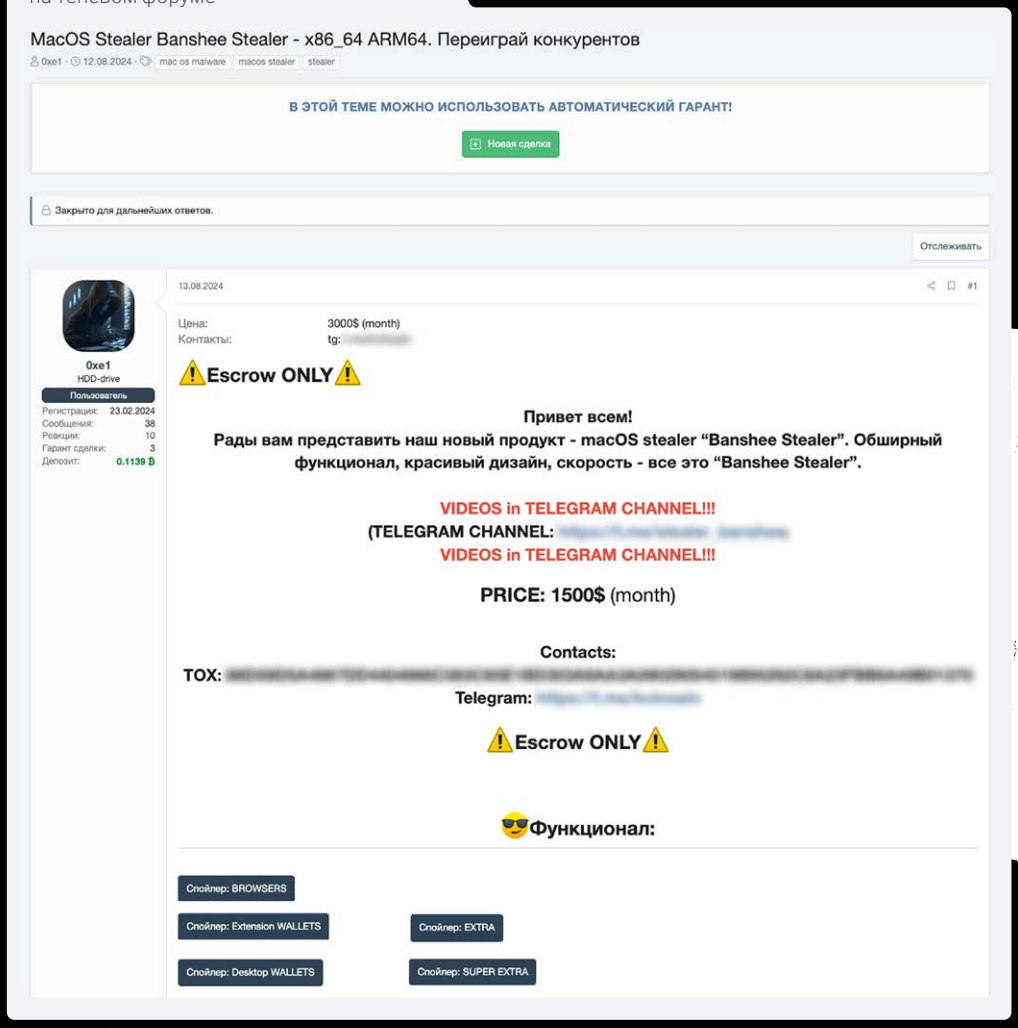
Тактика	Техника	Процедура
Execution	Command and Scripting Interpreter: Visual Basic	MetaStealer может быть собран в виде VBS-скрипта
	Command and Scripting Interpreter: JavaScript	MetaStealer может быть собран в виде JS-скрипта
Defense Evasion	Execution Guardrails	MetaStealer поддерживает блокировку по стране, билду и IP-адресу
	Obfuscated Files or Information: Binary Padding	MetaStealer может быть собран с увеличенным размером исполняемого файла для обхода средств защиты информации
	Obfuscated Files or Information: Encrypted/ Encoded File	MetaStealer использует шифрование строк с помощью алгоритмов AES256 и XOR
	Obfuscated Files or Information: Junk Code Insertion	MetaStealer использует фейковый нативный код

Тактика	Техника	Процедура
Credential Access	Credentials from Password Stores: Credentials from Web Browsers	MetaStealer извлекает данные учетных записей браузеров
Collection	Automated Collection	MetaStealer автоматически осуществляет сбор данных в системе
	Clipboard Data	MetaStealer получает текстовые данные из буфера обмена
	Data from Local System	MetaStealer собирает различные данные из скомпрометированной системы (Telegram, Discord, FTP, VPN, криптокошельки)
	Screen Capture	MetaStealer способен создавать снимки экрана рабочего стола
Discovery	System Location Discovery	MetaStealer определяет географическое расположение жертвы с целью предотвратить запуск на территории России
	System Owner/User Discovery	MetaStealer получает имена пользователя и компьютера
Exfiltration	Automated Exfiltration	MetaStealer автоматически отправляет собранные с компьютера жертвы данные на сервер атакующих
	Exfiltration Over C2 Channel	MetaStealer отправляет собранные с компьютера жертвы данные на сервер атакующих

Banshee Stealer

Banshee Stealer — стилер для macOS, представленный на одном из теневых форумов. Его стоимость составляет 1500 $ в месяц, что объясняется редкостью подобных решений для этой операционной системы. macOS менее распространена и обладает повышенной защитой от нелегитимных действий.

Объявление о продаже Banshee Stealer на теневом форуме



В Banshee Stealer — стандартные для подобного ПО функции по сбору конфиденциальных данных. Стилер способен извлекать логины и пароли, похищать cookie-сессии, работать с популярными браузерами и криптовалютными кошельками — как в виде браузерных расширений, так и в качестве самостоятельных приложений.

Дополнительно стилер собирает информацию из системных заметок, связки ключей и другие системные данные. Собранные логи и уведомления можно отправлять непосредственно в Telegram.

MITRE ATT&CK

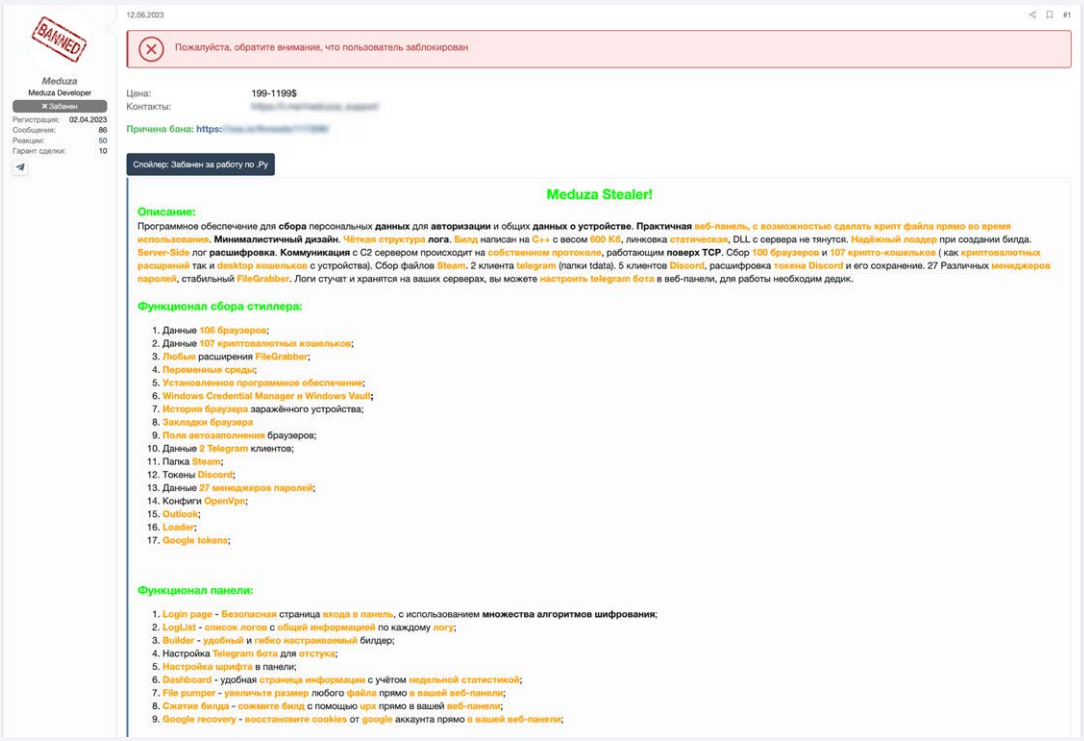
Тактика	Техника	Процедура
Defense Evasion	Hide Artifacts: Hidden Window	Banshee Stealer скрывает окно консоли при запуске
Credential Access	Credentials from Password Stores: Keychain	Banshee Stealer извлекает данные учетных записей Keychain
	Credentials from Password Stores: Credentials from Web Browsers	Banshee Stealer извлекает данные учетных записей браузеров
	OS Credential Dumping	Banshee Stealer получает пароль macOS
	Steal Web Session Cookie	Banshee Stealer получает cookie-файлы браузеров: Safari, Chrome, Firefox, Brave, Edge, Vivaldi, Yandex, Opera, Opera GX
Collection	Automated Collection	Banshee Stealer автоматически осуществляет сбор данных в системе
	Data from Local System	Banshee Stealer собирает различные данные в скомпрометированной системе, например заметки и данные криптокошельков
Discovery	System Information Discovery	Banshee Stealer собирает информацию о скомпрометированной системе
Exfiltration	Automated Exfiltration	Banshee Stealer автоматически отправляет собранные с компьютера жертвы данные на сервер атакующих
	Exfiltration Over Web Service	Banshee Stealer использует Telegram API для отправки собранных на компьютере жертвы данных

Meduza Stealer

Meduza Stealer — зрелый стилер с широкой функциональностью, от кражи данных браузеров и криптокошельков до перехвата токенов Google и учетных записей Discord. За 199 $ в месяц, помимо функций стилера, пользователь получает еще и загрузчик.

За $ 199 в месяц, помимо функций стилера, пользователь получает еще и загрузчик.

Объявление о продаже Meduza Stealer на теневом форуме



На скриншоте показано относительно старое объявление. С тех пор разработчик регулярно выпускал обновления: к середине 2024 года вышло более пяти версий.

Стилер использует собственный протокол для связи с C2-сервером, что усложняет обнаружение этого ВПО системами защиты.

Судя по описанию, Meduza Stealer собирает данные:

- из 100+ браузеров и 100+ криптокошельков;
- популярных менеджеров паролей;
- почтовых клиентов;
- файлов пользователя;
- Telegram и Discord;
- системных компонентов Windows (установленное ПО, хранилище учетных данных).

Административная панель отличается высоким уровнем проработки и включает в себя защиту стартовой страницы, настраиваемый билдер и дашборд с детальной статистикой за выбранный период. Кроме того, в интерфейсе панели предусмотрена возможность восстановления cookie-файлов аккаунта Google.

MITRE ATT&CK

Тактика	Техника	Процедура
Defense Evasion	Obfuscated Files or Information	Meduza Stealer может быть зашифрован при сборке в веб-панели
	Obfuscated Files or Information: Binary Padding	Meduza Stealer может быть собран с увеличенным размером исполняемого файла для обхода средств защиты информации
	Obfuscated Files or Information: Software Packing	Meduza Stealer может быть упакован UPX
	Virtualization/Sandbox Evasion	Meduza Stealer определяет запуск в виртуальной машине или песочнице

Тактика	Техника	Процедура
Credential Access	Credentials from Password Stores	Meduza Stealer извлекает данные учетных записей Outlook
	Credentials from Password Stores: Credentials from Web Browsers	Meduza Stealer извлекает данные учетных записей браузеров
	Credentials from Password Stores: Windows Credential Manager	Meduza Stealer извлекает данные учетных записей Windows Credential Manager и Windows Vault
	Credentials from Password Stores: Password Managers	Meduza Stealer извлекает данные учетных записей менеджеров паролей
Collection	Automated Collection	Meduza Stealer автоматически осуществляет сбор данных в системе
	Data from Local System	Meduza Stealer собирает различные данные в скомпрометированной системе (Telegram, Discord, Steam, OpenVPN, криптокошельки), а также файлы с определенными расширениями
Discovery	File and Directory Discovery	Meduza Stealer использует модуль FileGrabber для поиска файлов по определенным расширениям
	Software Discovery	Meduza Stealer получает информацию об установленном ПО в скомпрометированной системе
	System Owner/User Discovery	Meduza Stealer получает имена пользователя и компьютера через переменные среды
Command and Control	Non-Application Layer Protocol	Meduza Stealer использует собственный протокол поверх TCP для коммуникации с управляющим сервером
Exfiltration	Automated Exfiltration	Meduza Stealer автоматически отправляет собранные с компьютера жертвы данные на сервер атакующих
	Exfiltration Over C2 Channel	Meduza Stealer отправляет собранные с компьютера жертвы данные на сервер атакующих

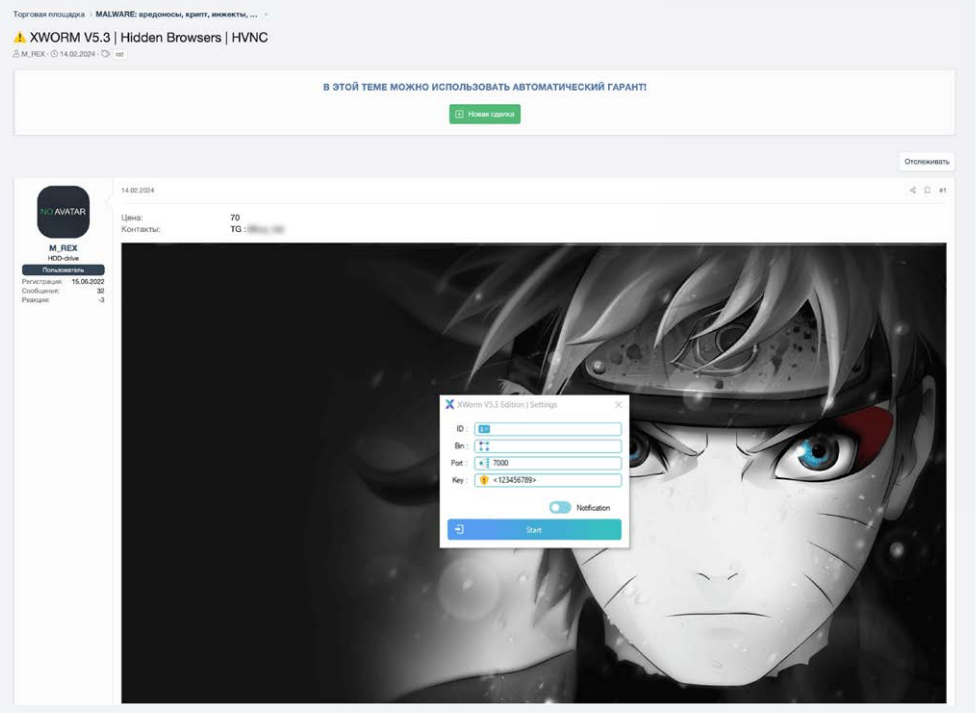
Трояны удаленного доступа (RAT)

XWorm

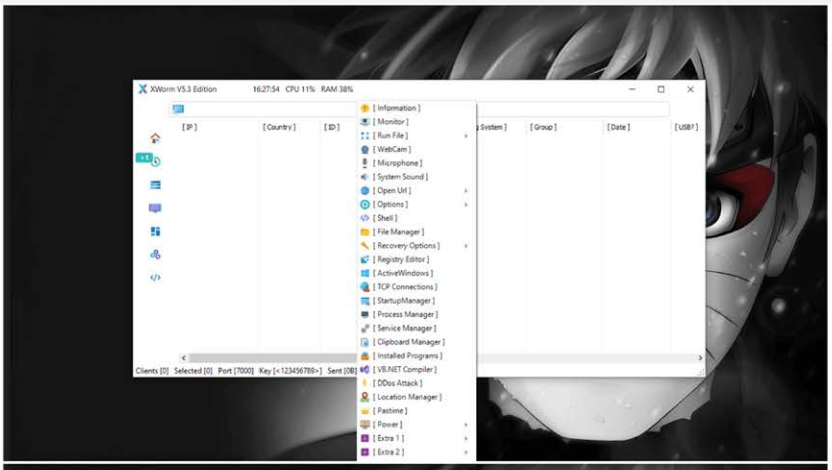
XWorm — троян для удаленного доступа. Несмотря на относительно низкую цену (около 70 $), на теневых форумах, на GitHub и в телеграм-каналах часто встречаются взломанные версии разной степени актуальности.

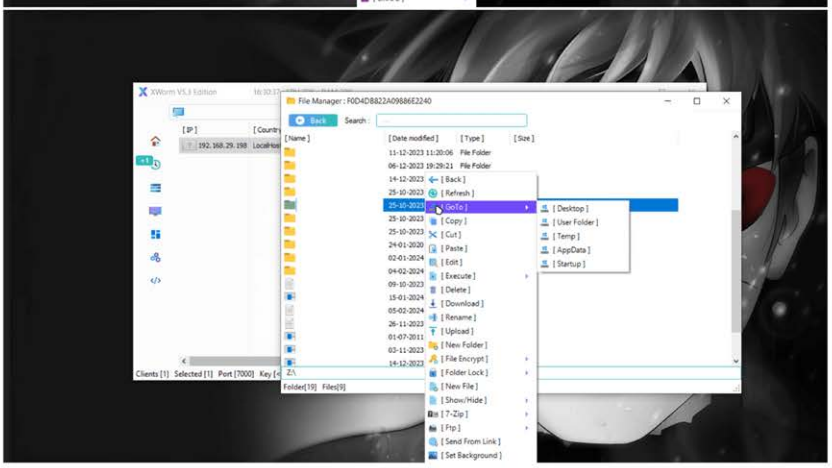
Около $70 на теневых форумах.

Объявление о продаже трояна XWorm на теневом форуме



Объявление о продаже трояна XWorm на теневом форуме





⭐ Password Recovery :

✅ | Passwords - Cookies - CreditCards - Bookmarks - Downloads - Keywords - History - Autofill |
✅ | All-In-One - Discord Tokens - TelegramSession - ProductKey - MetaMask - InternetExplorer - FileZilla - Wifi Keys |

⭐ Extra Tools :

✅ | Fud Downloader [HTA] - Icon Changer - Multi Binder [Icon - Assembly - Obfuscator] |

⭐ Hidden RDP
⭐ Hidden Browser (Chrome | Brave | Firefox | Edge)
⭐ Hidden RDP
⭐ Reverse Proxy
⭐ UAC Bypass [RunAs - Cmstp - Fodhelper]
⭐ Invoke-BSOD
⭐ Ngrok Installer
⭐ Bot killer
⭐ WDKiller
⭐ WDDisable
⭐ WDExclusion and More ...

⚙ Requirements :

🔸 .Net Framework 4.5 [Controller]
🔸 .Net Framework 4.0 [Client]

🌟 Price : 70$ (1 PC Per Licence)

TG : [redacted]
TG Group : [redacted]

Вложения

QHcDaLrS.cleaned.png

⚠ Жалоба

👍 Like +Цитата ↩Ответ

В объявлении на скриншоте выше предлагается «официальная» версия программы.

Разработчик, стремясь подчеркнуть ключевые возможности решения, в заголовке делает акцент на функции создания виртуальных рабочих столов и скрытого запуска браузеров.

Набор утилит включает средства закрепления в системе: обход UAC, удаление конкурирующего ВПО, а также отключение и добавление в исключения Windows Defender.

XWorm обладает функциональностью стилера и умеет собирать:

- сохраненные пароли, cookie, данные кредитных карт, историю загрузок;
- сессии Telegram и Discord;
- данные MetaMask;
- Wi-Fi-ключи;
- данные из FTP-клиента FileZilla и другие.

Кроме того, вместе с трояном поставляется загрузчик, а также установщик легитимной утилиты ngrok для туннелирования трафика.

Простой интерфейс и низкая стоимость делают XWorm популярным среди технически не подготовленных злоумышленников, увеличивая риски успешных атак на корпоративные сети и личные устройства.

MITRE ATT&CK

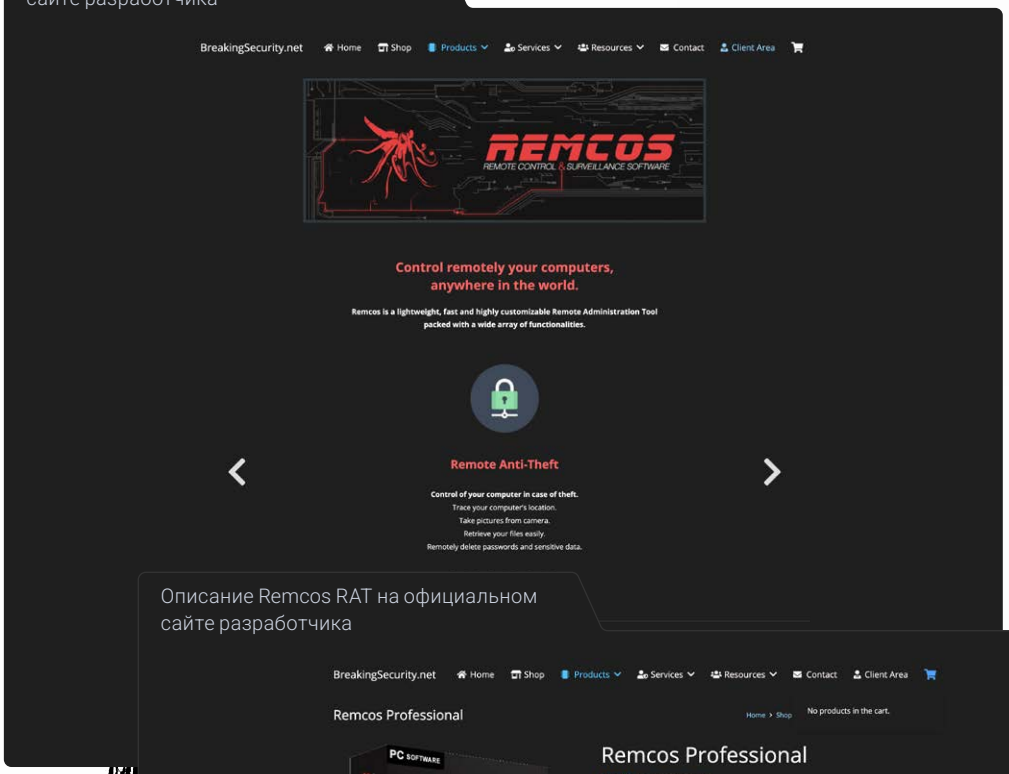
Тактика	Техника	Процедура
Defense Evasion	Abuse Elevation Control Mechanism: Bypass User Account Control	XWorm позволяет обойти UAC через runas, cmstp и fodhelper
	Impair Defenses: Disable or Modify Tools	XWorm может отключить Windows Defender или добавить файл в его исключения
	Hide Artifacts: Hidden Window	XWorm может запускать браузер, а также предоставлять доступ по RDP в скрытом режиме
	Masquerading	XWorm может быть замаскирован под легитимный файл
Credential Access	Credentials from Password Stores: Credentials from Web Browsers	XWorm позволяет извлечь сохраненные учетные данные из браузеров
	Unsecured Credentials	XWorm позволяет извлечь сохраненные учетные данные из файлов, реестра и т. п.
Lateral Movement	Remote Services: Remote Desktop Protocol	XWorm позволяет подключаться к скомпрометированной системе по RDP
Command and Control	Proxy	XWorm может инсталлировать ngrok для проксирования сетевых соединений
Impact	Service Stop	XWorm может завершать процессы и службы, относящиеся к другому ВПО

Remcos RAT

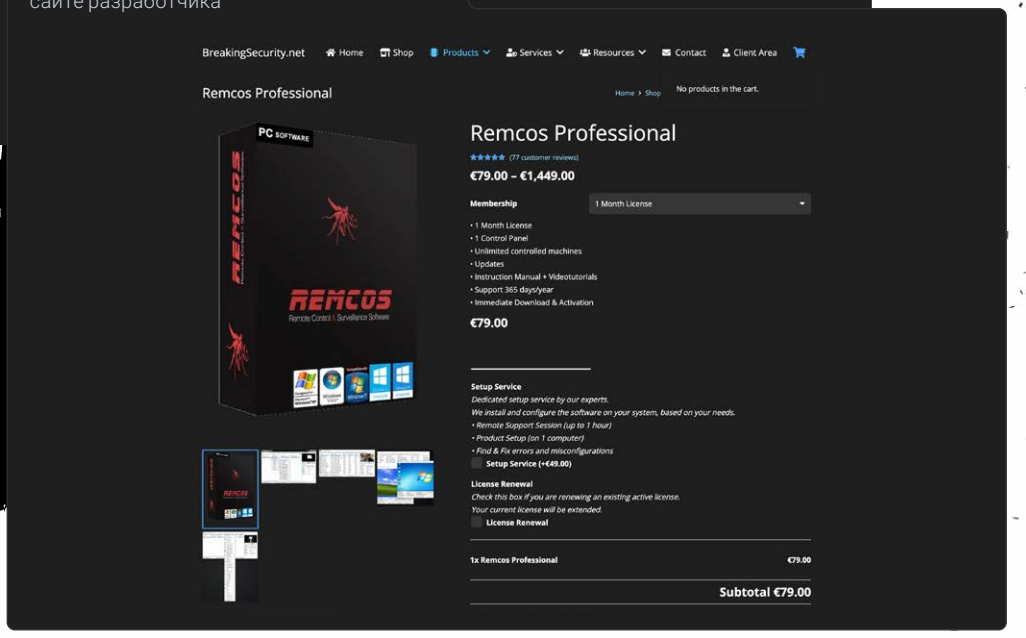
Remcos RAT — многофункциональный инструмент для удаленного администрирования, как его позиционирует официальный сайт разработчика Remcos Professional. Это коммерческий продукт с гибкой системой лицензирования — от 79 € в месяц до 1449 € за расширенные версии.

От € 79 в месяц
до € 1449
за расширенные версии.

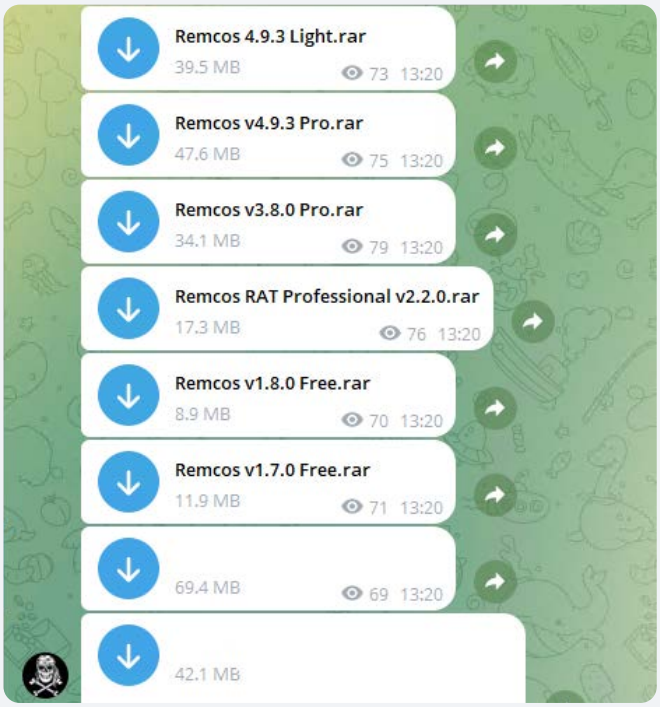
Описание Remcos RAT на официальном сайте разработчика



Описание Remcos RAT на официальном сайте разработчика



Файлы для загрузки Remcos RAT
в телеграм-канале злоумышленников



Основной акцент в описании сделан на легальности использования, однако исследователи киберугроз регулярно фиксируют множество атак с применением этого инструмента. Кроме того, на теневых форумах и в телеграм-чатах можно встретить многочисленные обсуждения его эксплуатации.

Функциональность Remcos очевидно рассчитана на скрытую работу в системе без ведома пользователя. Об этом свидетельствуют такие возможности:

- скрытый режим работы;
- кейлоггинг (фиксация нажатий клавиш);
- запись с микрофона и веб-камеры;
- remote shell и remote scripting;
- скрытая загрузка и исполнение файлов;
- удаление следов активности и конфиденциальных данных.

Таким образом, некоторые производители ВПО могут маскироваться под легитимных разработчиков, распространяя свои программы официальными способами.

MITRE ATT&CK

На основе официального руководства пользователя Remcos RAT можно выделить ряд техник MITRE ATT&CK.

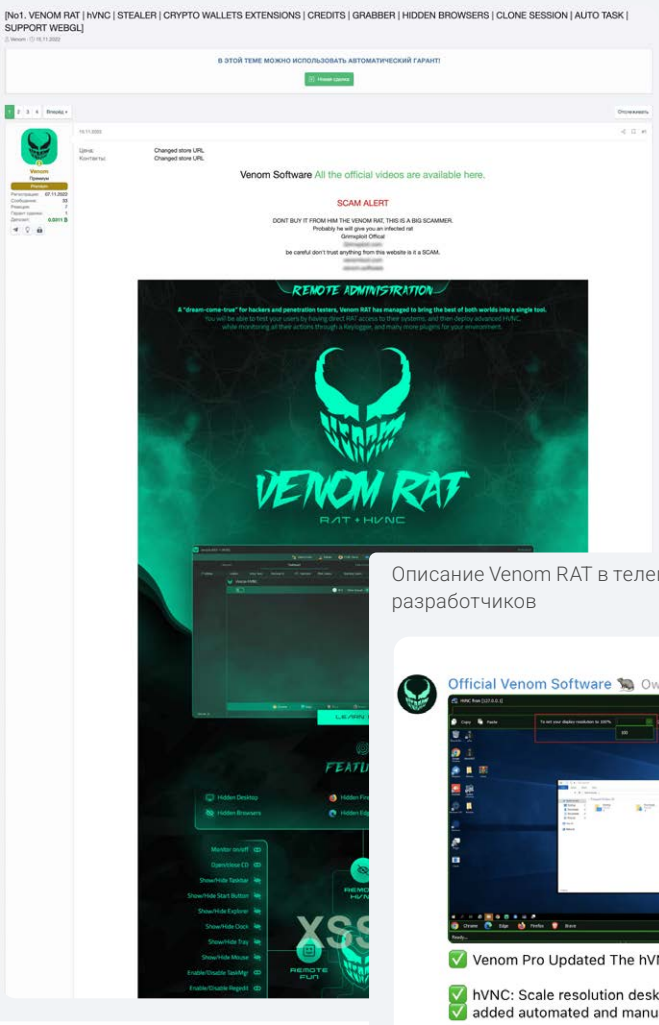
Тактика	Техника	Процедура
Execution	Command and Scripting Interpreter: Windows Command Shell	Remcos RAT предоставляет удаленный доступ к интерпретатору `cmd.exe`. Remcos RAT позволяет удаленно выполнять Batch-скрипты
	Command and Scripting Interpreter: JavaScript	Remcos RAT позволяет удаленно выполнять скрипты VBScript и JavaScript
Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Remcos RAT закрепляется в автозагрузке системы через ключ реестра Run
Defense Evasion	Hide Artifacts: Hidden Window	Remcos RAT может быть запущен без отображения окна программы и иконки в области уведомлений
	Modify Registry	Remcos RAT позволяет вносить изменения в реестр ОС
Credential Access	Credentials from Password Stores	Remcos RAT получает пароли, хранящиеся в файлах различных программ на скомпрометированном хосте
Collection	Audio Capture	Remcos RAT получает доступ к микрофону скомпрометированного хоста
	Data from Local System	Remcos RAT собирает историю браузеров
	Input Capture: Keylogging	Remcos RAT использует модуль кейлоггера
	Screen Capture	Remcos RAT создает снимки экрана рабочего стола
	Video Capture	Remcos RAT получает доступ к веб-камере скомпрометированного хоста

Тактика	Техника	Процедура
Discovery	File and Directory Discovery	Remcos RAT использует модуль файлового менеджера для работы с файловой системой скомпрометированного хоста
	Process Discovery	Remcos RAT получает список запущенных процессов в системе
	System Network Configuration Discovery	Remcos RAT получает IP-адрес скомпрометированного хоста
Command and Control	Encrypted Channel: Asymmetric Cryptography	Remcos RAT использует TLS для шифрования соединения с управляющим сервером
	Non-Application Layer Protocol	Remcos RAT связывается с управляющим сервером по TCP
	Ingress Tool Transfer	Remcos RAT позволяет загружать дополнительные файлы на скомпрометированный хост с управляющего сервера
	Proxy	Remcos RAT использует скомпрометированный хост в качестве SOCKS5-прокси (прямой и обратный режимы)
	Web Service: Bidirectional Communication	Remcos RAT поддерживает возможность управления с помощью телеграм-бота
Impact	Data Destruction	Remcos RAT позволяет удаленно удалять файлы, а также очищать cookie-файлы и сохраненные пароли в браузерах на хосте жертвы

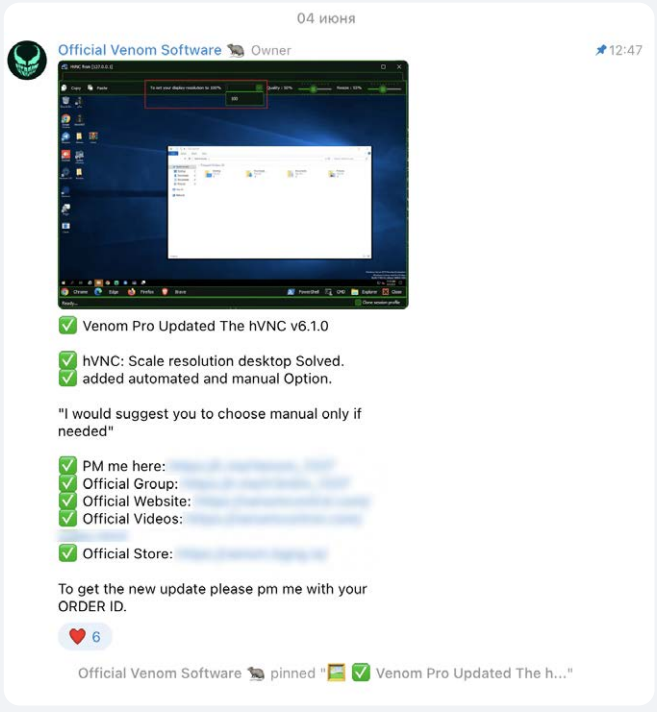
Venom RAT

Venom RAT — многофункциональный инструмент для удаленного администрирования, распространяемый через теневые форумы и телеграм-каналы.

Объявление о продаже Venom RAT на теневом форуме



Описание Venom RAT в телеграм-канале разработчиков



На скриншоте представлено объявление за 2022 год, однако ВПО продолжает активно развиваться: в телеграм-канале разработчика есть записи об обновлениях от июня 2025 года.

В описании особый акцент сделан на функциях скрытности:

- управлении видимостью элементов интерфейса (панель задач, меню «Пуск», часы, системный трей, курсор);
- скрытом режиме запуска браузеров (Chrome, Edge, Firefox, Internet Explorer);
- работе с файловой системой и реестром Windows;
- обходе системных защитных механизмов — отключении диспетчера задач, редактора реестра и Windows Defender.

Также реализована возможность выполнять автоматические задачи, управлять TCP-соединениями, мониторить активность и контролировать аппаратные компоненты.

Разработчики позиционируют Venom RAT как «мечту хакера и пентестера», однако распространение через теневые каналы делает это ПО сомнительным инструментом в руках этичных хакеров.

MITRE ATT&CK

Тактика	Техника	Процедура
Execution	Command and Scripting Interpreter: Windows Command Shell	Venom RAT предоставляет удаленный доступ к интерпретатору командной строки
Persistence	Boot or Logon Autostart Execution	Venom RAT закрепляется в автозагрузке системы
Privilege Escalation	Abuse Elevation Control Mechanism: Bypass User Account Control	Venom RAT позволяет обходить UAC (User Account Control)
Defense Evasion	Hide Artifacts: Hidden Window	Venom RAT использует модуль HVNC (Hidden Virtual Network Computing) для скрытной работы с браузерами, проводником и рабочими столами
	Impair Defenses: Disable or Modify Tools	Venom RAT способен отключать Windows Defender
	Modify Registry	Venom RAT позволяет вносить изменения в реестр ОС

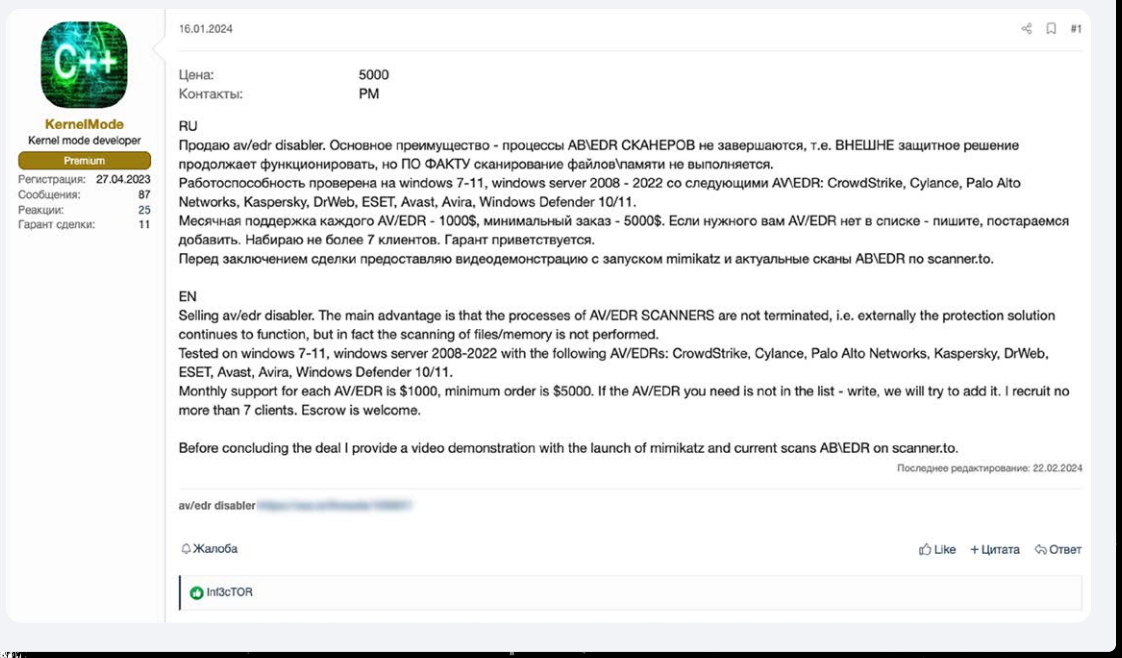
Тактика	Техника	Процедура
Credential Access	Credentials from Password Stores	Venom RAT получает пароли, хранящиеся в файлах различных программ на скомпрометированном хосте
	Credentials from Password Stores: Credentials from Web Browsers	Venom RAT способен собирать сохраненные в браузерах пароли
	Steal Web Session Cookie	Venom RAT способен собирать cookie-файлы из браузеров
Lateral Movement	Remote Services	Venom RAT использует модуль HVNC (Hidden Virtual Network Computing) для удаленного доступа к системе
Collection	Audio Capture	Venom RAT получает доступ к микрофону и позволяет вести аудиозапись с устройства
	Automated Collection	Venom RAT автоматически собирает различные данные на скомпрометированном хосте
	Data from Local System	Venom RAT собирает токены Discord
	Input Capture: Keylogging	Venom RAT использует модуль кейлоггера
	Video Capture	Venom RAT получает доступ к веб-камере скомпрометированного хоста
Discovery	File and Directory Discovery	Venom RAT использует модуль файлового менеджера для работы с файловой системой скомпрометированного хоста
	System Information Discovery	Venom RAT собирает информацию о скомпрометированной системе
Command and Control	Non-Application Layer Protocol	Venom RAT связывается с управляющим сервером по TCP
	Ingress Tool Transfer	Venom RAT позволяет загружать дополнительные файлы на скомпрометированный хост с управляющего сервера
Exfiltration	Automated Exfiltration	Venom RAT автоматически передает собранные с хоста данные на сервер управления
	Exfiltration Over C2 Channel	Venom RAT передает собранные со скомпрометированного хоста данные на управляющий сервер

EDR- и AV-киллеры

AV/EDR Disabler от KernelMode

AV/EDR Disabler — специализированный инструмент для подавления защитных решений, который продавец KernelMode предлагает на теневых форумах.

Объявление о продаже AV/EDR Disabler от пользователя KernelMode на теневом форуме



В объявлении ВПО представлено как коммерческая услуга с индивидуальным подходом. Основной акцент сделан на скрытой деактивации защитных механизмов: процессы антивирусов и EDR-систем сохраняют видимость работы, но фактически перестают выполнять проверки.

Такой подход создает иллюзию безопасности зараженной системы, что позволяет закрепиться в ней на долгий срок.

Разработчик заявляет о поддержке широкого спектра решений — от корпоративных (CrowdStrike, Palo Alto, Cylance) до потребительских (Avast, Avira, ESET, Windows Defender).

Эффективность инструмента подтверждается демонстрацией запуска mimikatz и тестами на актуальных базах scanner.to. Это говорит о том, что киллер релевантен современным механизмам обнаружения.

Условия распространения:

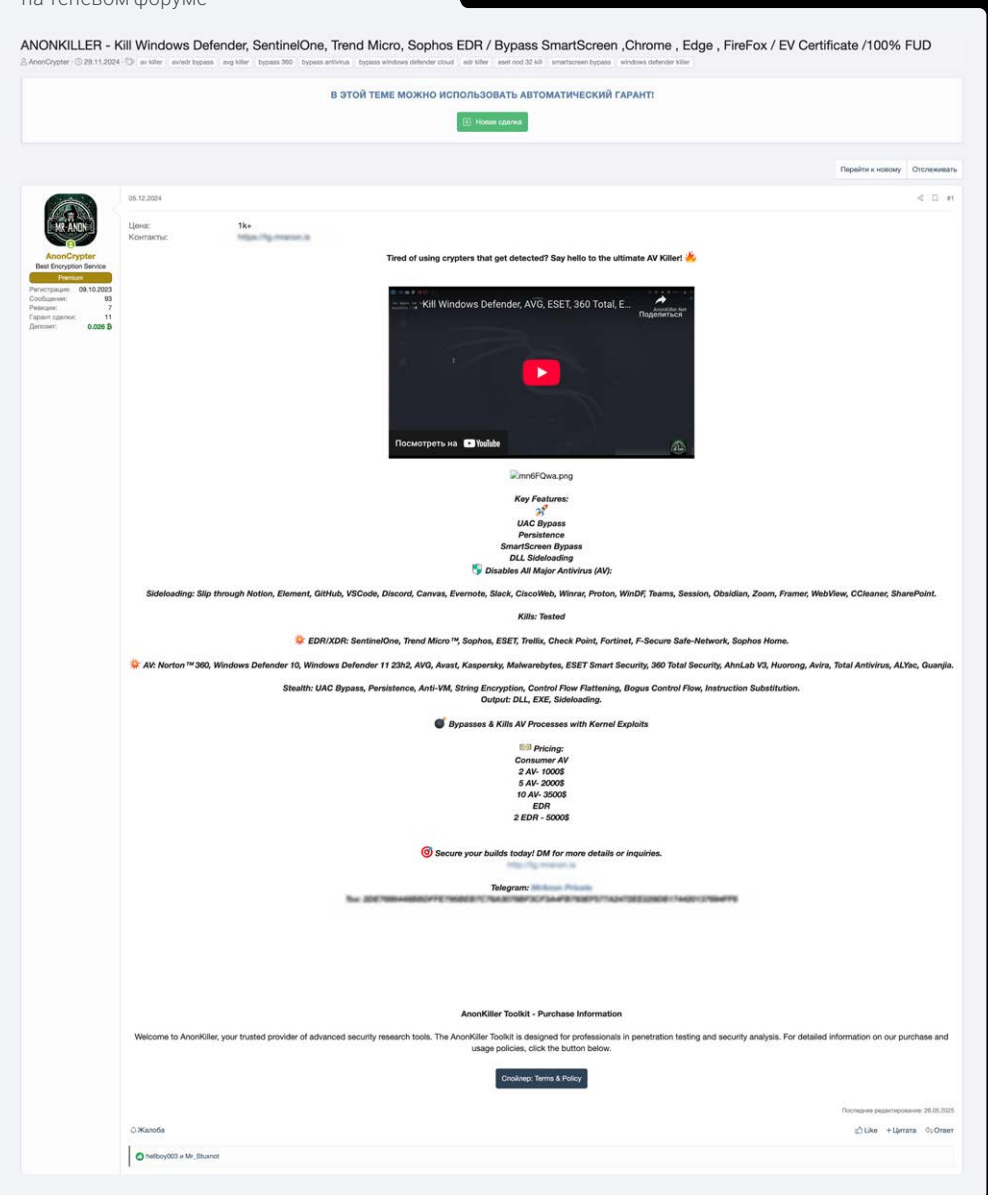
- Работа не более чем с 7 клиентами одновременно.
- Поддержка конкретных AV/EDR — от 1000 $ в месяц, минимальный заказ — 5000 $.

Такая модель продаж может указывать на использование инструмента в целевых атаках, а не в массовых кампаниях.

AnonKiller Toolkit

AnonKiller — комплексный инструмент, который подавляет защитные решения. Позиционируется как «решение для пентестеров», но фактически предназначен для скрытого отключения антивирусов, EDR- и XDR-систем.

Объявление о продаже AnonKiller на теневом форуме



В объявлении разработчик делает акцент на полном обходе защитных механизмов, например UAC и SmartScreen, а также на загрузке вредоносного кода через DLL sideloading.

В списке решений, на которых опробовали ВПО, — как массовые продукты вроде Windows Defender, Kaspersky и Norton, так и корпоративные EDR- и XDR-решения, включая SentinelOne, Sophos, Trend Micro и Check Point.

AnonKiller поддерживает различные форматы исполняемых файлов: EXE, DLL, а также предоставляет необходимые файлы для реализации sideloading, позволяя злоумышленнику гибко адаптировать вектор атаки под конкретную целевую систему.

Модель лицензирования варьируется в зависимости от количества целевых защитных решений:

- 1000 $ — за поддержку двух антивирусов;
- 3000 $ — за десять AV-продуктов;
- 5000 $ — за два EDR-решения.

Такая ценовая политика указывает на ориентацию инструмента на целевые атаки, а не на массовое распространение.

MITRE ATT&CK

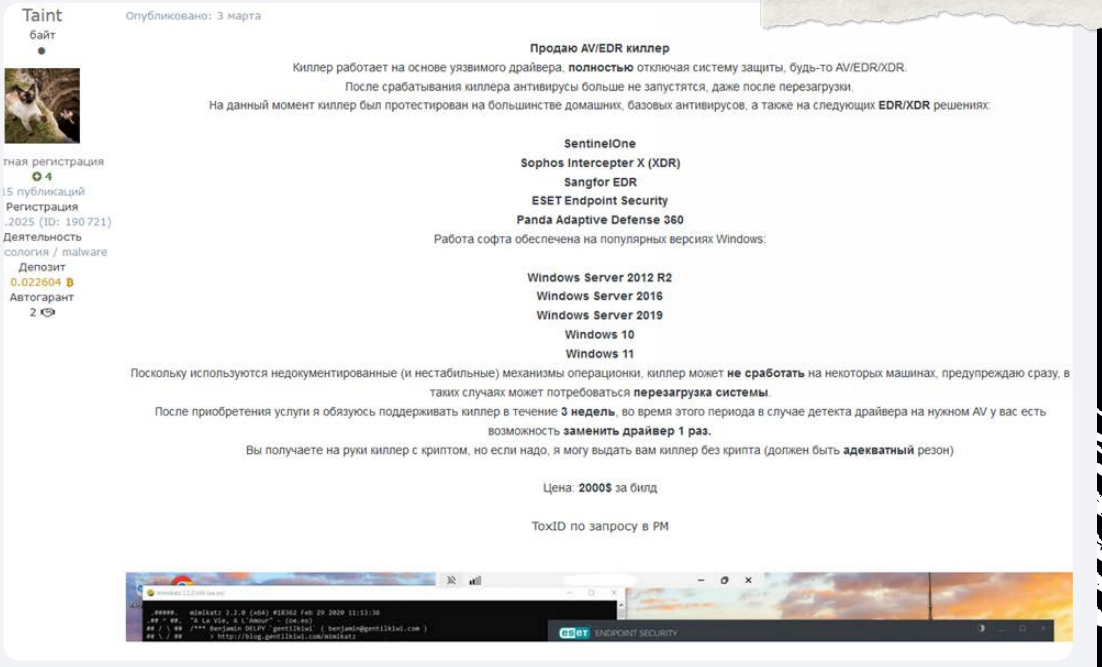
Тактика	Техника	Процедура
Persistence	Boot or Logon Autostart Execution	AnonKiller закрепляется в автозагрузке системы
Privilege Escalation	Abuse Elevation Control Mechanism: Bypass User Account Control	AnonKiller позволяет обходить UAC (User Account Control)
Defense Evasion	Hijack Execution Flow: DLL	AnonKiller использует DLL sideloading для запуска вредоносной библиотеки
	Impair Defenses: Disable or Modify Tools	AnonKiller отключает средства антивирусной защиты: Norton 360, Defender в Windows 11 23H2, AVG, Avast, Kaspersky, Malwarebytes, ESET Smart Security, 360 Total Security, AhnLab V3, Huorong, Avira, Total Antivirus, ALYac, Guanjia
	Obfuscated Files or Information	AnonKiller использует шифрование строк, обфускацию кода control flow flattening
	Obfuscated Files or Information: Junk Code Insertion	AnonKiller использует «мусорный» код
	Subvert Trust Controls: Mark-of-the-Web Bypass	AnonKiller способен обходить SmartScreen
	Virtualization/Sandbox Evasion	AnonKiller проверяет запуск в виртуальной среде

EDR- и AV-киллер от Taint

EDR- и AV-киллер от Taint — инструмент для обхода защитных решений, доступный в виде индивидуального варианта для каждого пользователя. Предлагается на одном из теневых форумов за фиксированную стоимость — 2000 $.

Предлагается на одном из теневых форумов за фиксированную стоимость — $ 2000

Объявление о продаже EDR- и AV-киллера от пользователя Taint на теневом форуме



Taint
байт

тная регистрация
4
15 публикаций
Регистрация
.2025 (ID: 190 721)
Деятельность
сология / malware
Депозит
0.022604 ₿
Автогарант
2

Опубликовано: 3 марта

Продаю AV/EDR киллер

Киллер работает на основе уязвимого драйвера, **полностью** отключая систему защиты, будь-то AV/EDR/XDR.
После срабатывания киллера антивирусы больше не запустятся, даже после перезагрузки.
На данный момент киллер был протестирован на большинстве домашних, базовых антивирусов, а также на следующих **EDR/XDR** решениях:

SentinelOne
Sophos Intercepter X (XDR)
Sangfor EDR
ESET Endpoint Security
Panda Adaptive Defense 360

Работа софта обеспечена на популярных версиях Windows:

Windows Server 2012 R2
Windows Server 2016
Windows Server 2019
Windows 10
Windows 11

Поскольку используются недокументированные (и нестабильные) механизмы операционки, киллер может **не сработать** на некоторых машинах, предупреждаю сразу, в таких случаях может потребоваться **перезагрузка системы**.
После приобретения услуги я обязуюсь поддерживать киллер в течение **3 недель**, во время этого периода в случае детекта драйвера на нужном AV у вас есть возможность **заменить драйвер 1 раз.**
Вы получаете на руки киллер с криптом, но если надо, я могу выдать вам киллер без крипта (должен быть **адекватный** резон)

Цена: **2000$** за билд

ToxID по запросу в PM

Разработчик заявляет, что инструмент использует уязвимый драйвер. Это позволяет полностью отключать системы AV, EDR, XDR на уровне ядра, включая блокировку повторного запуска даже после их перезагрузки.

Функциональность протестирована на современных корпоративных решениях, включая SentinelOne, Sophos Intercept X, ESET Endpoint, Panda Adaptive Defense и другие, а также на большинстве популярных домашних антивирусов. Заявлена совместимость с Windows 10, 11 и серверными ОС вплоть до 2019 года, однако отмечается нестабильность работы из-за использования недокументированных функций системы. В некоторых случаях для активации эффекта может потребоваться ручная перезагрузка.

Модель распространения ограничена: клиент получает инструмент с криптованием (по умолчанию), а техническая поддержка предоставляется в течение трех недель с возможностью однократной замены драйвера, если инструмент будет обнаружен защитными механизмами. По договоренности доступна опция получить вариант ПО без предварительного криптования.

Высокая цена и индивидуальный подход к сопровождению указывают на то, что продукт ориентирован на узкий круг операторов со специализацией на целевых атаках.

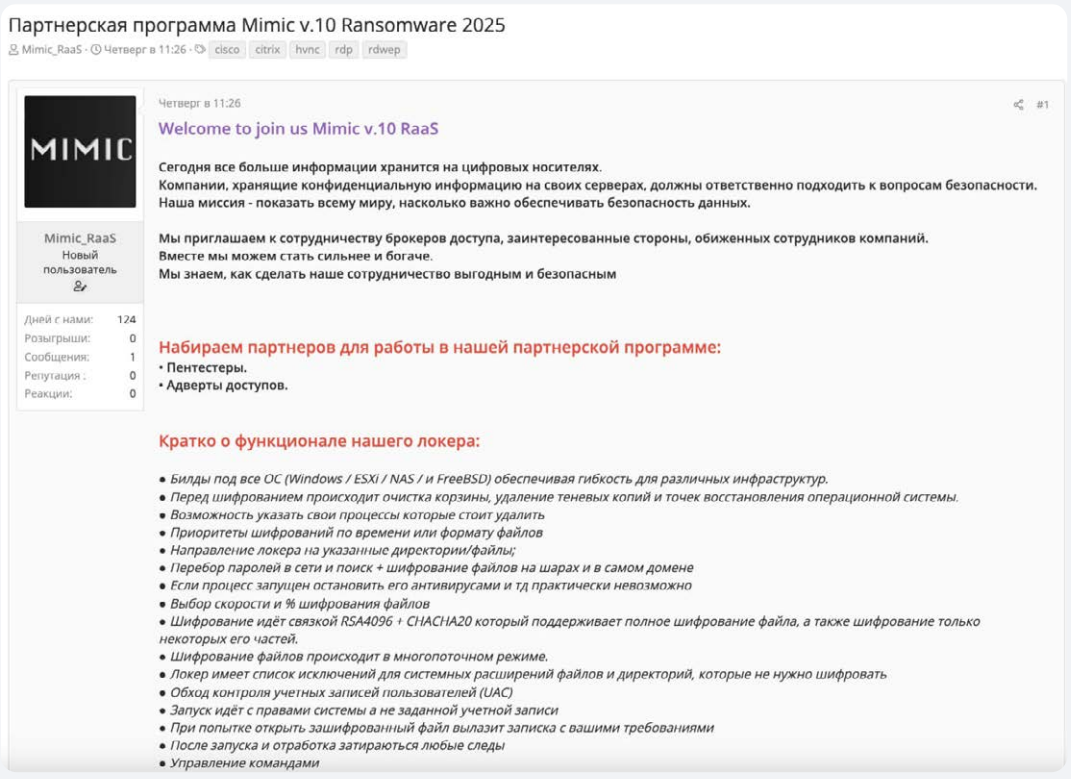
Программы-вымогатели

Экосистема программ-вымогателей в России и СНГ отличается от западной как по характеру атак, так и по используемым инструментам. В международной практике часто применяются известные RaaS-сервисы (такие как LockBit или REvil), а в России злоумышленники обычно обходятся без них. Вместо этого они используют либо собственные решения, либо модифицированные билдеры, ранее утекшие в сеть. Например, в 2023 году мы рассказывали об атаках с использованием утекших билдеров Babuk, LockBit и Conti.

Mimic Ransomware

Mimic Ransomware v.10 — шифровальщик, распространяемый по модели RaaS и ориентированный на участников теневого рынка, включая брокеров доступов и инсайдеров.

Объявление о продаже шифровальщика Mimic на теневом форуме



Партнерская программа Mimic v.10 Ransomware 2025

Mimic_RaaS · Четверг в 11:26 · cisco citrix hvnc rdp rdwep

MIMIC

Mimic_RaaS
Новый пользователь

Дней с нами: 124
Розыгрыши: 0
Сообщения: 1
Репутация: 0
Реакции: 0

Четверг в 11:26 #1

Welcome to join us Mimic v.10 RaaS

Сегодня все больше информации хранится на цифровых носителях.
Компании, хранящие конфиденциальную информацию на своих серверах, должны ответственно подходить к вопросам безопасности.
Наша миссия - показать всему миру, насколько важно обеспечивать безопасность данных.

Мы приглашаем к сотрудничеству брокеров доступа, заинтересованные стороны, обиженных сотрудников компаний.
Вместе мы можем стать сильнее и богаче.
Мы знаем, как сделать наше сотрудничество выгодным и безопасным

Набираем партнеров для работы в нашей партнерской программе:
• Пентестеры.
• Адверты доступов.

Кратко о функционале нашего локера:

• Билды под все ОС (Windows / ESXi / NAS / и FreeBSD) обеспечивая гибкость для различных инфраструктур.
• Перед шифрованием происходит очистка корзины, удаление теневых копий и точек восстановления операционной системы.
• Возможность указать свои процессы которые стоит удалить
• Приоритеты шифрований по времени или формату файлов
• Направление локера на указанные директории/файлы;
• Перебор паролей в сети и поиск + шифрование файлов на шарах и в самом домене
• Если процесс запущен остановить его антивирусами и тд практически невозможно
• Выбор скорости и % шифрования файлов
• Шифрование идёт связкой RSA4096 + CHACHA20 который поддерживает полное шифрование файла, а также шифрование только некоторых его частей.
• Шифрование файлов происходит в многопоточном режиме.
• Локер имеет список исключений для системных расширений файлов и директорий, которые не нужно шифровать
• Обход контроля учетных записей пользователей (UAC)
• Запуск идёт с правами системы а не заданной учетной записи
• При попытке открыть зашифрованный файл выпадет записка с вашими требованиями
• После запуска и отработка затираються любые следы
• Управление командами

Разработчики делают упор на гибкость и устойчивость решения: доступны билды под Windows, NAS, FreeBSD и ESXi, что позволяет применять ВПО в разнородных корпоративных инфраструктурах.

Предлагаемое ПО позволяет настраивать приоритеты шифрования по времени и типу файлов, запускать процессы с правами SYSTEM в обход UAC, а также автоматически завершать заданные процессы — это снижает вероятность вмешательства защитного ПО.

Шифрование построено на связке RSA-4096 и ChaCha20. Поддерживаются как полное, так и частичное шифрование с использованием многопоточности. Инструмент настроен так, чтобы не затрагивать критически важные для работы ОС файлы и папки, минимизируя риск нарушения ее работоспособности.

Дополнительные функции включают перебор паролей в сети и шифрование сетевых папок, что расширяет зону поражения. После выполнения задачи вымогатель самостоятельно удаляет следы своей активности.

Коммерческие условия, включая стоимость и размер комиссии, не раскрываются.

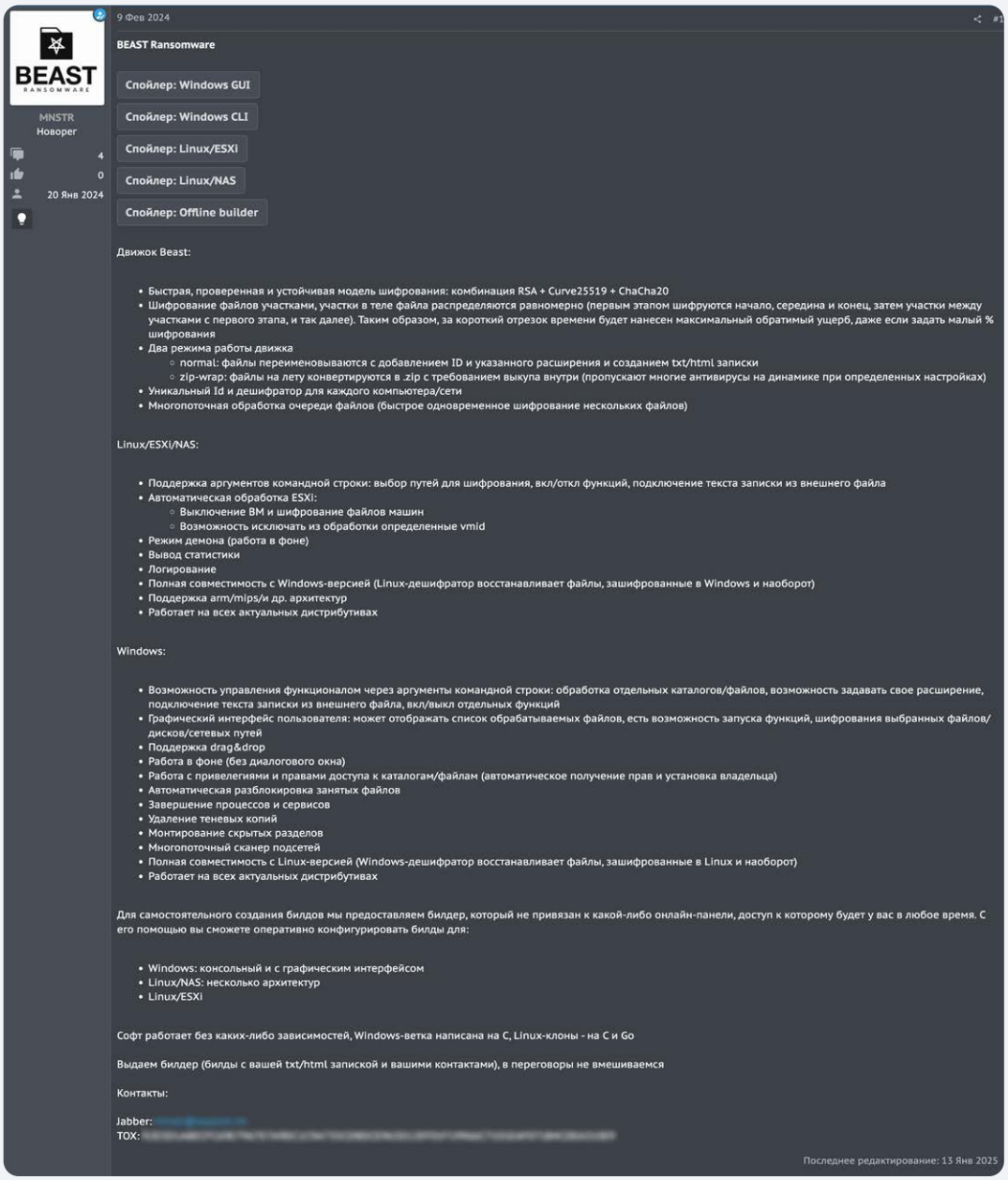
MITRE ATT&CK

Тактика	Техника	Процедура
Privilege Escalation	Abuse Elevation Control Mechanism: Bypass User Account Control	Mimic позволяет обходить UAC (User Account Control)
Defense Evasion	Indicator Removal	Mimic удаляет следы своей активности после запуска
Credential Access	Brute Force	Mimic осуществляет перебор паролей в сети
Discovery	File and Directory Discovery	Mimic содержит список исключений для системных файлов и каталогов, которые не следует шифровать
Impact	Data Destruction	Mimic удаляет содержимое «Корзины»
	Data Encrypted for Impact	Mimic шифрует данные на диске, а также на общих сетевых ресурсах и в домене
	Inhibit System Recovery	Mimic удаляет теневые копии и точки восстановления ОС

Beast Ransomware

Beast Ransomware — вымогатель с поддержкой Windows, Linux, NAS и ESXi, ориентированный на гибкость шифрования и стабильную работу в различных средах.

Объявление о продаже Beast Ransomware на теневом форуме



9 Фев 2024

BEAST Ransomware

Спойлер: Windows GUI

Спойлер: Windows CLI

Спойлер: Linux/ESXi

Спойлер: Linux/NAS

Спойлер: Offline builder

MNSTR
Новорег
4
0
20 Янв 2024

Движок Beast:

- Быстрая, проверенная и устойчивая модель шифрования: комбинация RSA + Curve25519 + ChaCha20
- Шифрование файлов участками, участки в теле файла распределяются равномерно (первым этапом шифруются начало, середина и конец, затем участки между участками с первого этапа, и так далее). Таким образом, за короткий отрезок времени будет нанесен максимальный обратимый ущерб, даже если задать малый % шифрования
- Два режима работы движка
  - normal: файлы переименовываются с добавлением ID и указанного расширения и созданием txt/html записки
  - zip-wrap: файлы на лету конвертируются в .zip с требованием выкупа внутри (пропускают многие антивирусы на динамике при определенных настройках)
- Уникальный Id и дешифратор для каждого компьютера/сети
- Многопоточная обработка очереди файлов (быстрое одновременное шифрование нескольких файлов)

Linux/ESXi/NAS:

- Поддержка аргументов командной строки: выбор путей для шифрования, вкл/откл функций, подключение текста записки из внешнего файла
- Автоматическая обработка ESXi:
  - Выключение ВМ и шифрование файлов машин
  - Возможность исключать из обработки определенные vmid
- Режим демона (работа в фоне)
- Вывод статистики
- Логирование
- Полная совместимость с Windows-версией (Linux-дешифратор восстанавливает файлы, зашифрованные в Windows и наоборот)
- Поддержка arm/mips/и др. архитектур
- Работает на всех актуальных дистрибутивах

Windows:

- Возможность управления функционалом через аргументы командной строки: обработка отдельных каталогов/файлов, возможность задавать свое расширение, подключение текста записки из внешнего файла, вкл/выкл отдельных функций
- Графический интерфейс пользователя: может отображать список обрабатываемых файлов, есть возможность запуска функций, шифрования выбранных файлов/дисков/сетевых путей
- Поддержка drag&drop
- Работа в фоне (без диалогового окна)
- Работа с привелегиями и правами доступа к каталогам/файлам (автоматическое получение прав и установка владельца)
- Автоматическая разблокировка занятых файлов
- Завершение процессов и сервисов
- Удаление теневых копий
- Монтирование скрытых разделов
- Многопоточный сканер подсетей
- Полная совместимость с Linux-версией (Windows-дешифратор восстанавливает файлы, зашифрованные в Linux и наоборот)
- Работает на всех актуальных дистрибутивах

Для самостоятельного создания билдов мы предоставляем билдер, который не привязан к какой-либо онлайн-панели, доступ к которому будет у вас в любое время. С его помощью вы сможете оперативно конфигурировать билды для:

- Windows: консольный и с графическим интерфейсом
- Linux/NAS: несколько архитектур
- Linux/ESXi

Софт работает без каких-либо зависимостей, Windows-ветка написана на C, Linux-клоны - на C и Go

Выдаем билдер (билды с вашей txt/html запиской и вашими контактами), в переговоры не вмешиваемся

Контакты:

Jabber:
TOX:

Последнее редактирование: 13 Янв 2025

Разработчик уделяет особое внимание скорости, обратимости ущерба и обходу антивирусных решений.

Движок шифрования сочетает алгоритмы RSA, Curve25519 и ChaCha20, используя каскадную сегментированную логику: сначала шифруются критически важные участки файлов, затем промежуточные. Это позволяет нанести значительный ущерб даже при частичном шифровании.

Доступны два режима работы:

- Классический — с изменением расширений файлов и генерацией записок с требованиями.
- ZIP-wrap — с архивированием файлов и размещением внутри требований, чтобы их было сложнее обнаружить (защитными механизмами).

Версия для Linux/ESXi поддерживает работу в демон-режиме, управление через аргументы командной строки и взаимодействие с виртуальными машинами, включая их остановку и последующее шифрование.

Windows-версия реализована с графическим интерфейсом, поддерживает drag & drop, многопоточную обработку, мониторинг скрытых разделов, удаление теневых копий и автоматическое получение прав доступа к файлам.

Отдельный билдер позволяет генерировать исполняемые файлы с учетом целевой ОС и архитектуры. Решение не требует подключения к онлайн-панели, что минимизирует операционные риски.

Кросс-платформенная совместимость дешифраторов между Windows и Linux подчеркивает зрелость продукта и его широкую применимость в различных сценариях.

MITRE ATT&CK

Тактика	Техника	Процедура
Execution	Command and Scripting Interpreter: Windows Command Shell	Beast Ransomware управляется через командную строку, позволяя задавать расширения, путь, запуск функций и т. д.
	Command and Scripting Interpreter: Unix Shell	Версия Beast Ransomware для Linux/ESXi поддерживает shell-интерфейс для управления шифрованием
Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Версия Beast Ransomware для Windows может обеспечивать автозапуск за счет прописывания своих компонентов в автозагрузку
Defense Evasion	Obfuscated Files or Information	Beast Ransomware обфусцирован для минимизации возможностей обнаружения
	Indicator Removal on Host: File Deletion	Beast Ransomware может удалять следы своей активности
Impact	Inhibit System Recovery	Beast Ransomware удаляет теневые копии
	Service Stop	Beast Ransomware останавливает службы и завершает процессы
	Data Encrypted for Impact	Beast Ransomware шифрует файлы с использованием комбинации RSA + Curve25519 + ChaCha20

ВПО, которое используют для атак на компании в России и СНГ

Киберггруппировки, использующие коммерческое ВПО (MaaS) и активные с 2024 г.

1. Cavalry Werewolf
2. Cobalt Werewolf
3. Dirty Wolf
4. Fluffy Wolf
5. Gambling Hyena
6. Lenient Wolf
7. Lone Wolf
8. Lucky Werewolf
9. Pandemonium Hyena
10. Rare Werewolf
11. Ravage Wolf
12. Romantic Wolf
13. Scaly Wolf
14. Shadow Wolf
15. Sticky Werewolf
16. Stone Wolf
17. Twelfth Hyena
18. Venture Wolf

Загрузчики

DarkGate: Cobalt Werewolf, Stone Wolf, Shadow Wolf

Стилеры

1. Rhadamanthys Stealer: Sticky Werewolf, Rare Werewolf
2. Formbook: Ravage Wolf, Romantic Wolf
3. SnakeKeylogger: Ravage Wolf, Romantic Wolf
4. RedLine: Ravage Wolf
5. MetaStealer: Venture Wolf, Fluffy Wolf, Sticky Werewolf, Lucky Werewolf
6. Atomic Stealer
7. Lumma Stealer: Sticky Werewolf
8. Webrat
9. Nova
10. White Snake: Scaly Wolf
11. Meduza Stealer: Stone Wolf, Lucky Werewolf
12. Poseidon Stealer
13. Banshee Stealer
14. MacStealer

Трояны удаленного доступа (RAT)

1. zgRAT: Fluffy Wolf

2. Warzone RAT: Cavalry Werewolf, Fluffy Wolf

3. NetWire RAT: Gorgon Werewolf

4. Remcos: Gorgon Werewolf, Stone Wolf, Romantic Wolf, Sticky Werewolf

5. DarkCrystal

6. DarkGate: Cobalt Werewolf, Ravenous Wolf, Stone Wolf, Shadow Wolf

7. NanoCore RAT: Gorgon Werewolf

8. BurnsRAT: Fluffy Wolf

9. RADX RAT

10. Ozone RAT: Sticky Werewolf

11. XWorm: Monolithic Werewolf, Romantic Wolf

12. njRAT: Gorgon Werewolf, Translucent Werewolf, Wanted Werewolf, Key Wolf, Romantic Wolf

13. EkipaRAT: Cobalt Werewolf

Программы-вымогатели

1. LockBit (полученный с помощью билдера): Lone Wolf, Gambling Hyena, Lenient Wolf, Dirty Wolf, Pandemonium Hyena, Twelfth Hyena, Shadow Wolf

2. AvosLocker

3. BlackBasta Ransomware: Ravenous Wolf

4. Zeppelin: Rigorous Wolf

Знания об особенностях ВПО, которое продается на теневых ресурсах, помогают компаниям получить представление об актуальном ландшафте угроз и усилить защиту. Мы рекомендуем использовать данные портала BI.ZONE Threat Intelligence, чтобы быть в курсе последних трендов.

Обфускация вредоносного программного обеспечения с помощью крипторов

В этой части исследования мы рассмотрим примеры объявлений об аренде крипторов и продаже услуг по криптованию файлов, а также цены на них.

Крипторы — это программное обеспечение, которое использует комбинацию шифрования, обфускации и манипуляции кода вредоносного программного обеспечения, что значительно затрудняет обнаружение этого ПО средствами защиты, а в некоторых случаях делает его полностью незаметным.

Различают публичные и приватные крипторы. Приватный криптор — это ограниченно распространяемый продукт, доступный лишь узкому кругу пользователей, благодаря чему ВПО, которое его использует, сложно детектировать. Публичный криптор, как следует из названия, доступен неограниченному кругу пользователей. Соответственно, использующие его вредоносные файлы обнаруживаются значительно быстрее. Но разработчики крипторов и поставщики услуг по криптованию регулярно обновляют свое программное обеспечение, чтобы поддерживать его недетектируемость.

Ценообразование в сегменте крипторов

На теневых ресурсах представлены объявления с предложением аренды самих крипторов и продажа услуг по криптованию файлов. В первом случае оплата взимается за период использования, например за месяц, а во втором — за каждый закриптованный файл.
В зависимости от способа продажи можно выделить следующие цены:

Подписка на криптор — от $79 в месяц.

Криптование файлов — от $30 за файл.

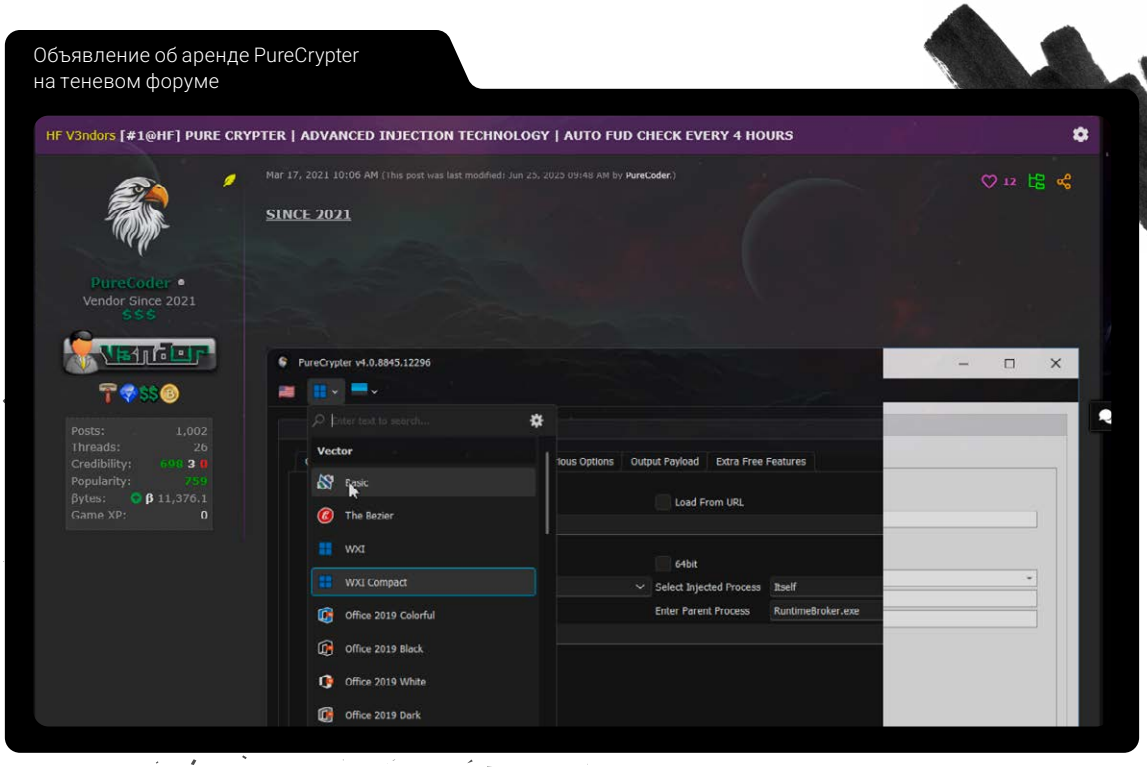
Крипторы

Ниже рассмотрим примеры крипторов, объявления о продаже которых мы обнаружили.

PureCrypter

PureCrypter — это популярный криптор, который активно используется различными злоумышленниками, в том числе нацеленными на организации в России и СНГ.

Объявление об аренде PureCrypter на теневом форуме



Автор объявления отмечает: чтобы поддерживать недектируемость криптора, его проверяют каждые 4 часа. Если более двух антивирусных средств обнаруживают криптор, он автоматически модифицируется.

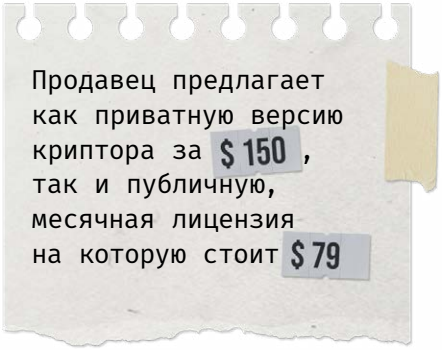
По заявлению продавца, криптор может выполнять функции загрузчика, а также имеет дополнительные функциональные возможности, например позволяет выполнять команды в PowerShell.

Также разработчик отмечает, что криптор имеет широкие возможности для противодействия анализу и средствам защиты, а именно:

- Модифицирует ETW (Event Tracing for Windows) и AMSI (Antimalware Scan Interface).
- Добавляет себя в исключения Windows Defender.
- Использует временные задержки при выполнении кода и ограничивает выполнение в виртуальных средах.
- При необходимости самоудаляется, изменяет временные метки, изолирует скомпрометированную систему от интернета, а также внедряется в легитимные процессы.

Криптор поддерживает добавление в автозагрузку, а также кастомизацию исполняемого файла, чтобы замаскировать его под легитимный.

Готовый файл может иметь расширения `.exe`, `.pif` или `.scr`.



MITRE ATT&CK

Тактика	Техника	Процедура
Execution	Command and Scripting Interpreter: PowerShell	PureCrypter может выполнять команды в PowerShell
Persistence	Boot or Logon Autostart Execution	PureCrypter может помещать вредоносный файл в автозагрузку
Defense Evasion	Debugger Evasion	PureCrypter использует техники антиотладки
	Impair Defenses: Disable or Modify Tools	PureCrypter модифицирует AMSI, добавляется в исключения Windows Defender
	Impair Defenses: Indicator Blocking	PureCrypter модифицирует ETW
	Indicator Removal: File Deletion	PureCrypter может самоудаляться
	Indicator Removal: Timestomp	PureCrypter может изменять значения временных меток
	Obfuscated Files or Information	PureCrypter обфусцирован для затруднения анализа и обнаружения
	Process Injection	PureCrypter внедряет код в другие процессы (x86/x64), используя режимы RunPE или LoadPE (шелл-код)
	Virtualization/Sandbox Evasion	PureCrypter проверяет запуск в виртуальной среде
	Virtualization/Sandbox Evasion: Time Based Evasion	PureCrypter использует временную задержку при выполнении
Command and Control	Application Layer Protocol: Web Protocols	PureCrypter использует HTTP/HTTPS для коммуникации с сервером
	Ingress Tool Transfer	PureCrypter может выполнять функцию загрузчика

Crypters & Tools

Crypters & Tools представлен не в объявлении на форуме, а на отдельном промолендинге. Подчеркивается, что Windows Defender и другие средства защиты не могут обнаружить это программное обеспечение.

Промолендинг Crypters & Tools

Автор отмечает, что злоумышленники широко используют его разработку, и приводит список ВПО, которое поддерживает криптор.

Продавец подчеркивает, что Crypters & Tools позволяет закрепляться в скомпрометированной системе сразу несколькими способами:

- через модификацию реестра (предположительно, Run) с помощью regedit;
- создание задачи в планировщике;
- добавление вредоносного файла в автозагрузку.

Криптор поставляется в разных форматах: VBS, JS, BAT и других.

Стоимость программного обеспечения — от $ 200 в день. При этом разработчик обещает ежедневные обновления, а также техническую поддержку 24/7.

MITRE ATT&CK

Тактика	Техника	Процедура
Execution	Command and Scripting Interpreter: Windows Command Shell	Crypters & Tools может поставляться в виде BAT-файла
	Command and Scripting Interpreter: Visual Basic	Crypters & Tools может поставляться в виде VBS-файла
	Command and Scripting Interpreter: JavaScript	Crypters & Tools может поставляться в виде JS-файла
Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Crypters & Tools может закрепляться в скомпрометированной системе посредством модификации реестра или папки автозагрузки
	Scheduled Task/Job: Scheduled Task	Crypters & Tools может закрепляться в скомпрометированной системе через создание задачи в планировщике
Defense Evasion	Obfuscated Files or Information	Crypters & Tools обфусцирован для затруднения анализа и обнаружения
	Obfuscated Files or Information: Encrypted/ Encoded File	Crypters & Tools шифрует вредоносную нагрузку, чтобы обойти средства защиты

Услуги по обфускации вредоносного кода и инструментов: примеры объявлений

Подобные услуги чаще всего предлагают на теневых форумах и в Telegram.

Asgard Protector Bot

Услугу по криптованию файлов предлагают через бота в Telegram.

Объявление об услуге криптования в Asgard Protector Bot

Asgard Protector Bot
bot

Asgard Protector (Support - @[redacted]
Бот для защиты ваших файлов.
Цена за один файл - **45$**
🟢 Каждый защищаемый файл накрывается уникальным стабом (автоматическая уникализация, каждый файл разный на ~90-95%).
🟢 Добавляет от 500 до 800кб (размер самого стаба) веса к файлу
🟢 Для того чтобы начать пользоваться ботом, нужно пополнить баланс, используйте команду /addprotects (пополнение через BTC и USDT TRC20)
🟢 Посмотреть баланс протектов можно с помощью команды /mybalance
🟢 Перед протектом файла можно посмотреть скан и количество детектов на последнем файле, сделанным ботом. Для этого введите команду /lastscan

📌 Дополнительный функционал:
🟢 **Startup**: Добавление автозагрузки в файл: автостарт после перезагрузки ПК (имя в автозагрузке генерируется автоматически)
🟢 **Anti-VM**: запретить запуск на виртуальных машинах
🟢 **Fake error**: при запуске откроется окно с ошибкой, работа файла продолжится как обычно
🟢 **Self-Delete**: удалить файл после запуска
🟢 **Run as admin**: готовый файл будет запускаться от имени администратора (может быть UAC окно!)
🟢 **Compatibility mode**: дополнительный режим работы, для совместимости с некоторыми файлами.
❗ Использовать только при указании на это саппорта ❗
🟢 **Pump the file size**: добавить дополнительный вес к файлу (Boost, pump file)
🟢 **Custom icon**: добавить на готовый файл вашу иконку (По умолчанию генерируется рандомная)
🟢 **Version info from exe**: Скопировать информацию о файле с другого exe
🟢 **Persistence**: добавить "неубиваемость" процесса в системе. При его закрытии он будет запускаться заново. Полезно если нужно чтобы файл держался в процессах как можно надежнее
🟢 **Iplogger**: добавить логгер к файлу, в который будет стучать файл при открытии. Нужно будет указать ссылку вида https: [redacted]
❗ ВАЖНО ❗ При использовании вашей иконки могут вылезать некоторые детекты. Пользуйтесь только качественными, проверенными иконками

После указания всех настроек и нажатия кнопки Protect, через определенное время вы получите готовый файл, запакованный в **zip** архив с паролем. И ссылку на скан с количеством детектов вида:
`Detects: 0`
`Scan link: https:` [redacted]

Автор подчеркивает уникальность каждого закриптованного файла, что затрудняет его детектируемость.

Сервис имеет дополнительные функциональные возможности, в частности позволяет:

- Использовать папку автозагрузки, чтобы закрепиться в скомпрометированной системе.
- Ограничивать запуск в виртуальных средах.
- Самоудаляться.
- Искусственно увеличивать размер файла для обхода средств защиты.
- Маскировать вредоносный файл под легитимный, модифицируя иконки и метаданные.
- Использовать IPLogger для сбора информации о скомпрометированной системе.

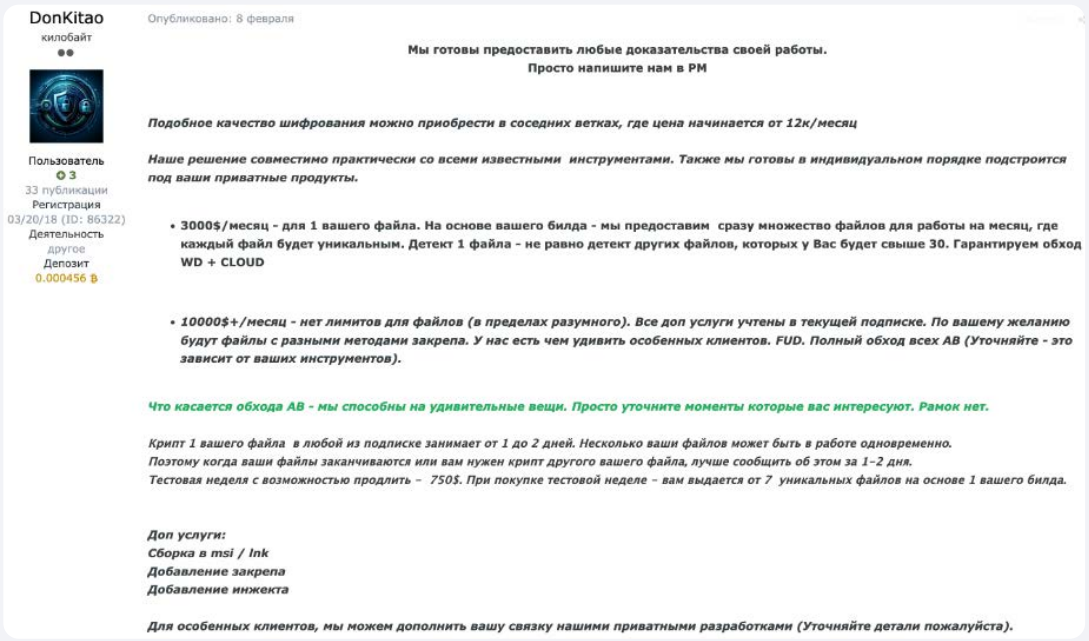
MITRE ATT&CK

Тактика	Техника	Процедура
Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Asgard Protector может закрепляться в скомпрометированной системе, используя папку автозагрузки
Defense Evasion	Obfuscated Files or Information	Asgard Protector обфусцирован для затруднения анализа и обнаружения
	Obfuscated Files or Information: Encrypted/ Encoded File	Asgard Protector шифрует вредоносную нагрузку для обхода средств защиты
	Indicator Removal: File Deletion	Asgard Protector может осуществлять самоудаление
	Obfuscated Files or Information: Binary Padding	Asgard Protector позволяет увеличить размер вредоносного файла, чтобы обойти средства защиты
	Virtualization/Sandbox Evasion	Asgard Protector проверяет запуск в виртуальной среде
	Masquerading	Asgard Protector позволяет использовать иконку и метаданные легитимного файла, чтобы замаскировать вредоносный
Discovery	System Information Discovery	Asgard Protector позволяет использовать сервис IPLogger для сбора информации о скомпрометированной системе

Криптование от DonKitao

В объявлении автор обещает доказать эффективность работы своего решения.

Объявление о криптовании от DonKitao на теневом форуме



DonKitao
килобайт
●●

Пользователь
✪ 3
33 публикации
Регистрация
03/20/18 (ID: 86322)
Деятельность
другое
Депозит
0.000456 ฿

Опубликовано: 8 февраля

Мы готовы предоставить любые доказательства своей работы.
Просто напишите нам в PM

Подобное качество шифрования можно приобрести в соседних ветках, где цена начинается от 12к/месяц

Наше решение совместимо практически со всеми известными инструментами. Также мы готовы в индивидуальном порядке подстроится под ваши приватные продукты.

- **3000$/месяц - для 1 вашего файла. На основе вашего билда - мы предоставим сразу множество файлов для работы на месяц, где каждый файл будет уникальным. Детект 1 файла - не равно детект других файлов, которых у Вас будет свыше 30. Гарантируем обход WD + CLOUD**

- ***10000$+/месяц - нет лимитов для файлов (в пределах разумного). Все доп услуги учтены в текущей подписке. По вашему желанию будут файлы с разными методами закрепа. У нас есть чем удивить особенных клиентов. FUD. Полный обход всех AB (Уточняйте - это зависит от ваших инструментов).***

Что касается обхода AB - мы способны на удивительные вещи. Просто уточните моменты которые вас интересуют. Рамок нет.

Крипт 1 вашего файла в любой из подписке занимает от 1 до 2 дней. Несколько ваши файлов может быть в работе одновременно.
Поэтому когда ваши файлы заканчиваются или вам нужен крипт другого вашего файла, лучше сообщить об этом за 1-2 дня.
Тестовая неделя с возможностью продлить - 750$. При покупке тестовой неделе - вам выдается от 7 уникальных файлов на основе 1 вашего билда.

Доп услуги:
Сборка в msi / lnk
Добавление закрепа
Добавление инжекта

Для особенных клиентов, мы можем дополнить вашу связку нашими приватными разработками (Уточняйте детали пожалуйста).

Продавец подчеркивает, что его продукт совместим с популярным ВПО, а также его можно адаптировать под собственные разработки злоумышленников.

Автор предлагает дополнительные возможности, например:

- Сборку в формате MSI или LNK.
- Закрепление в скомпрометированной системе.
- Внедрение в легитимные процессы.

Это предложение отличается по стоимости от аналогичных.

За **$ 3000** в месяц покупатель получит криптование одного файла, при этом клиенту предоставят более 30 таких файлов и гарантируют обход Windows Defender. Также предлагается вариант с неограниченным количеством файлов: его стоимость превышает **$10 000**.

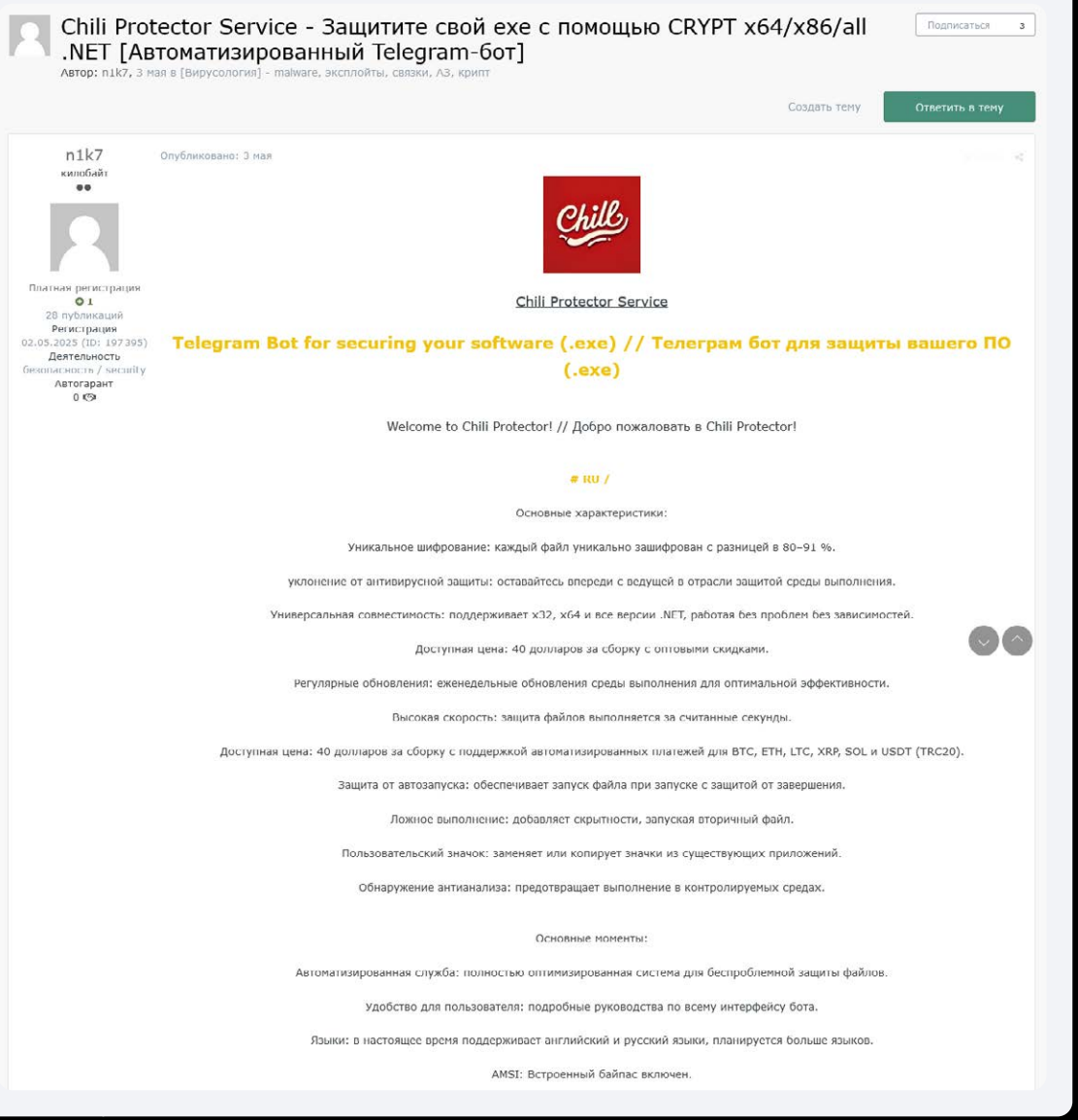
MITRE ATT&CK

Тактика	Техника	Процедура
Execution	User Execution: Malicious File	Пользователю необходимо открыть вредоносный LNK-файл, чтобы инициировать процесс компрометации
Defense Evasion	System Binary Proxy Execution: Msiexec	MSI-файл будет выполняться при помощи `msiexec.exe`
	Obfuscated Files or Information	Файл обфусцирован для затруднения анализа и обнаружения
	Obfuscated Files or Information: Encrypted/ Encoded File	Файл зашифрован для обхода средств защиты
	Process Injection	Может внедрять вредоносный код в легитимные процессы

Chili Protector Service

Сервис криптования файлов, который предоставляется через бота в Telegram.

Объявление о Chili Protector Service на теневом форуме



Chili Protector Service - Защитите свой exe с помощью CRYPT x64/x86/all .NET [Автоматизированный Telegram-бот]

Автор: n1k7, 3 мая в [Вирусология] - malware, эксплойты, связки, АЗ, крипт

Подписаться 3

Создать тему Ответить в тему

n1k7
килобайт

Платная регистрация
1
28 публикаций
Регистрация
02.05.2025 (ID: 197395)
Деятельность
безопасность / security
Автогарант
0

Опубликовано: 3 мая

Chili Protector Service

Telegram Bot for securing your software (.exe) // Телеграм бот для защиты вашего ПО (.exe)

Welcome to Chili Protector! // Добро пожаловать в Chili Protector!

RU /

Основные характеристики:

Уникальное шифрование: каждый файл уникально зашифрован с разницей в 80–91 %.

уклонение от антивирусной защиты: оставайтесь впереди с ведущей в отрасли защитой среды выполнения.

Универсальная совместимость: поддерживает x32, x64 и все версии .NET, работая без проблем без зависимостей.

Доступная цена: 40 долларов за сборку с оптовыми скидками.

Регулярные обновления: еженедельные обновления среды выполнения для оптимальной эффективности.

Высокая скорость: защита файлов выполняется за считанные секунды.

Доступная цена: 40 долларов за сборку с поддержкой автоматизированных платежей для BTC, ETH, LTC, XRP, SOL и USDT (TRC20).

Защита от автозапуска: обеспечивает запуск файла при запуске с защитой от завершения.

Ложное выполнение: добавляет скрытности, запуская вторичный файл.

Пользовательский значок: заменяет или копирует значки из существующих приложений.

Обнаружение антианализа: предотвращает выполнение в контролируемых средах.

Основные моменты:

Автоматизированная служба: полностью оптимизированная система для беспроблемной защиты файлов.

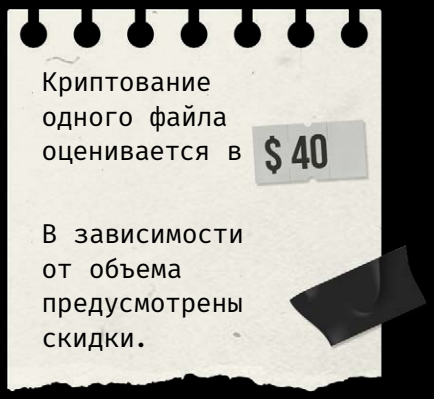
Удобство для пользователя: подробные руководства по всему интерфейсу бота.

Языки: в настоящее время поддерживает английский и русский языки, планируется больше языков.

AMSI: Встроенный байпас включен.

Продавец подчеркивает, что каждый файл зашифруется уникально: это снизит вероятность, что средства защиты быстро его обнаружат.

Сервис предоставляет как стандартные возможности (проверку запуска в виртуальной среде, маскировку под легитимные файлы и обход AMSI), так и более оригинальные — в частности, запуск дополнительного, вероятно легитимного, файла.



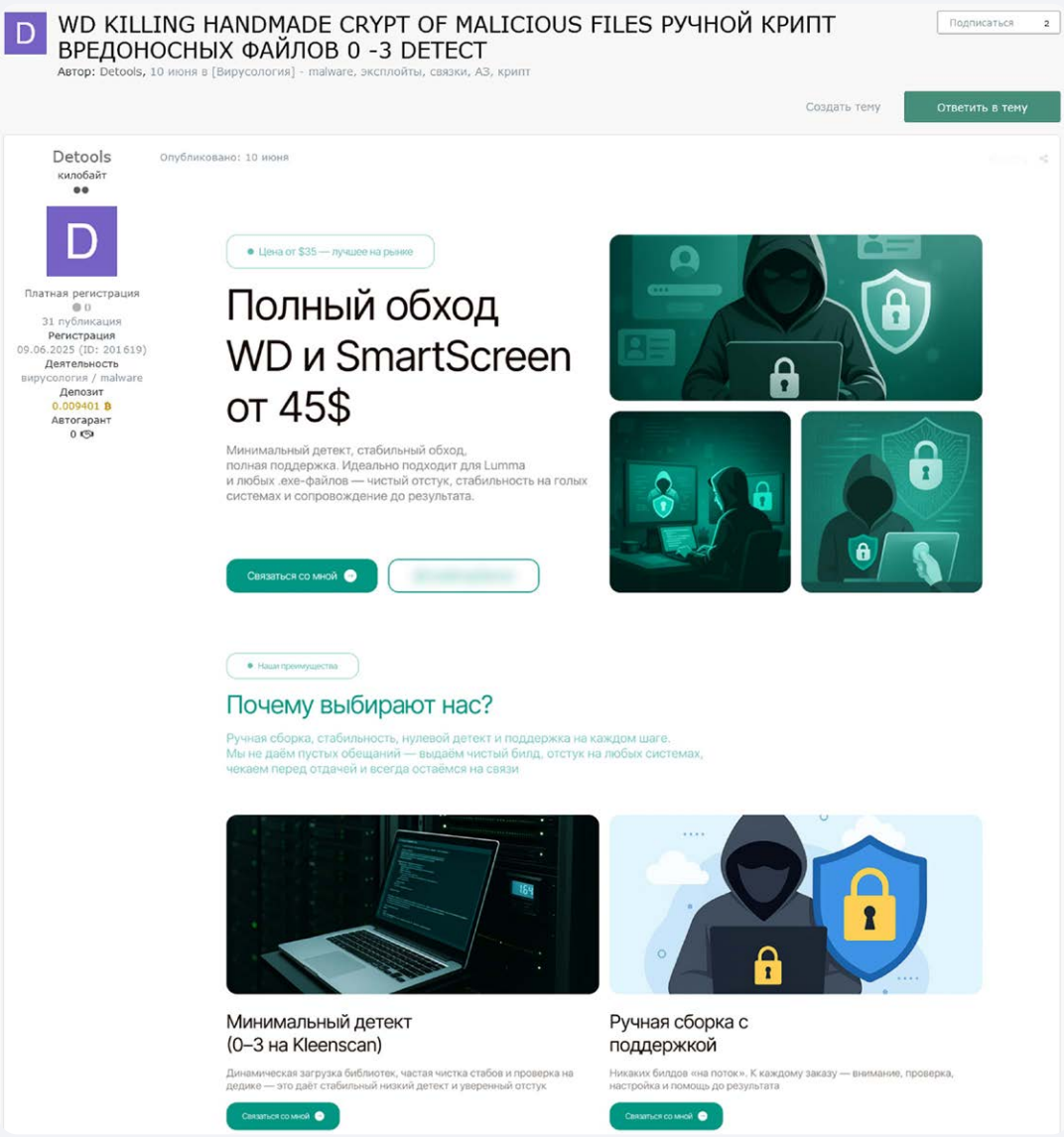
MITRE ATT&CK

Тактика	Техника	Процедура
Defense Evasion	Obfuscated Files or Information	Файл обфусцирован для затруднения анализа и обнаружения
	Obfuscated Files or Information: Encrypted/ Encoded File	Файл зашифрован для обхода средств защиты
	Virtualization/Sandbox Evasion	Проверяется запуск в виртуальной среде
	Masquerading	Может использоваться иконка легитимного файла, чтобы замаскировать вредоносный
	Impair Defenses: Disable or Modify Tools	Модифицируется AMSI
	Execution Guardrails	Может использоваться файл-пустышка или легитимный файл для обхода средств защиты

CrystalCrypt

Автор этого объявления предлагает услуги по криптованию вручную, отмечает минимальную обнаруживаемость файлов и регулярные обновления своих разработок.

Объявление о сервисе криптования CrystalCrypt на теневом форуме



Покупателям бесплатно доступны дополнительные функциональные возможности, а именно:

- Увеличение размера файла для обхода средств защиты.
- Объединение вредоносного файла с легитимным.
- Использование иконки легитимного файла.
- Добавление файла в автозагрузку.

MITRE ATT&CK

Тактика	Техника	Процедура
Persistence	Boot or Logon Autostart Execution	CrystalCrypt может добавить вредоносный файл в автозагрузку
Defense Evasion	Obfuscated Files or Information: Encrypted/ Encoded File	CrystalCrypt шифрует вредоносную нагрузку, чтобы обойти средства защиты
	Obfuscated Files or Information	CrystalCrypt обфусцирует файл для затруднения анализа и обнаружения
	Obfuscated Files or Information: Binary Padding	CrystalCrypt позволяет увеличить размер вредоносного файла, чтобы обойти средства защиты
	Obfuscated Files or Information: Embedded Payloads	CrystalCrypt позволяет объединить вредоносный файл с легитимным, чтобы обойти средства защиты
	Masquerading	CrystalCrypt позволяет использовать иконку легитимного файла, чтобы замаскировать вредоносный
	Impair Defenses: Disable or Modify Tools	CrystalCrypt может отключить Windows Defender

Уязвимости и эксплоиты

Помимо вредоносного программного обеспечения, на теневых форумах злоумышленники публикуют объявления об эксплоитах для различных уязвимостей. Эти предложения также пользуются большим спросом. На нелегальном рынке представлены как эксплоиты для 0-day-уязвимостей, так и для уже известных, у которых нет подходящих эксплоитов в открытых источниках.

Информация об уязвимостях, которые представляют интерес для злоумышленников, позволит своевременно устранить риски и приоритизировать ресурсы в рамках мониторинга IT-инфраструктуры организации.

Объявления о продаже эксплоитов для 0-day-уязвимостей

Подобные объявления довольно часто появляются на теневых ресурсах, но не всегда удается проверить их актуальность. Зачастую стоимость эксплоитов составляет сотни тысяч долларов, а в некоторых случаях может достигать нескольких миллионов.

Microsoft Office

В объявлении автор предлагает эксплоит для 0-day-уязвимости в Microsoft Office, которая позволяет выполнить команды в командной строке Windows или в PowerShell.

Автор просит за эксплоит $150 000 и предлагает продемонстрировать покупателю его работоспособность через сессию AnyDesk.

Объявление о продаже эксплоита для 0-day-уязвимости в Microsoft Office

NO AVATAR

malloc
bugzilla
Пользователь
Регистрация: 05.02.2020
Сообщения: 179
Реакции: 21

21.04.2024 Автор темы #24

[Продам] RCE MS office 0 дей

- Выполняется команда cmd/powershell
- Выполнение файлов exe, java, ps1, dll, другое... [ваши файлы должны быть чистыми, их можно и подписывать сертификатами в зависимости от файла, среднее выполнение пайлоада от 15 секунд до 1 минуты, все будет зависить от файла и его размера]
- Генератор уникальных хешей в документе [обеспечит долгую жизнь эксплоиту]
- Комплект: исходники, сборщик, описание уязвимости, мануал по установке и настройке этого "добра"
- Протестировано и работает на windows 7, 8, 10, 11.
- Уязвимые версии office: -> 2010 -> 2013 -> 2016 -> 2019 -> Office 365

- Скан АВ: 0/26

- Аверы, рессерчеры, и просто любопытные которые, не хотят покупать даже не пишите мне,я вас чувствую не тратьте мое время, а серьезно настроеному "баеру" мой ПМ - открыт!

- Все важные технические и рабочие моменты покажу "баеру", через AnyDesk и только при сделке.
- Контакты джаббер через ПМ, токс не использую!
- Гарант на покупателе обязательно!

- Цена 150.000$ оплата в битках/Monero, продажа в одни руки. Цену готов обсудить!

Авторизую контакты только после верефикации через ЛС форум

[*]- xo.

Жалоба Like + Цитата Ответ

Продавец отмечает, что на текущий момент (июль 2025 года) средства защиты не обнаруживают этот эксплоит. Тем не менее команды выполняются в популярных интерпретаторах. Это указывает на то, что вредоносную активность можно обнаружить на основе типичных поведенческих маркеров. В частности, выполнения команд и сценариев процессами, связанными с Microsoft Office.

TerraMaster NAS

Автор предлагает эксплоит сразу для трех уязвимостей, позволяющих удаленно выполнить произвольный код и получить root-права в системе TerraMaster NAS.

Объявление о продаже эксплоита для уязвимостей в TerraMaster NAS

Hi All,

Im selling TerraMaster preauth RCE

Item : TerraMaster NAS RCE
Target OS: linux x64
Required Privileges : No permissions required
Privileges Gained: Obtain root permissions of the NAS system
Number of Vulnerabilities: 3
Exploit Reliability : 100%
User Interaction : NO
Multi-versioning Support: TerraMaster 4 all versions, including the latest version || TerraMaster 5 All versions, including the latest.
Default Settings Compatibility: compatible

Deal over Forum Escrow is OK

Продавец отмечает, что эксплоит поддерживает даже последние версии программного обеспечения этого сетевого хранилища данных (network-attached storage, NAS). NAS содержат большой объем конфиденциальных данных или резервные копии, поэтому эти хранилища в первую очередь стараются удалить или зашифровать злоумышленники, распространяющие программы-вымогатели.

Получение аутентификационного материала

Продавец предлагает 0-day-эксплоит для получения аутентификационного материала, который позволит злоумышленнику реализовывать атаки типа pass-the-hash.

Объявление о продаже эксплоита, позволяющего получить аутентификационный материал

Цена:	2.5 BTC
Контакты:	Первый контакт в лс

Продам готовое самописное решение, для добычи NTLM-хешей.
0-day, 0-click. Юзверу не нужно делать никаких дополнительных действий либо кликов. Всё абсолютно скрытно.
Полностью самопис, полностью FUD 100%. На рынке такого нету!
Серверная часть и мануал входят в комплект.

Цена: 2.5 BTC

Демку не предоставляю. Только гарант.
Первый контакт - в ЛС.

Автор отмечает, что он самостоятельно разработал это ВПО и сейчас (в июле 2025 года) средства защиты не обнаруживают его. Также продавец предлагает руководство, как развернуть необходимую инфраструктуру и использовать программное обеспечение.

Межсетевой экран Palo Alto

На скриншоте ниже видно, что автор предлагает 0-day-эксплоит для уязвимости, позволяющей удаленно выполнить произвольный код на межсетевом экране Palo Alto.

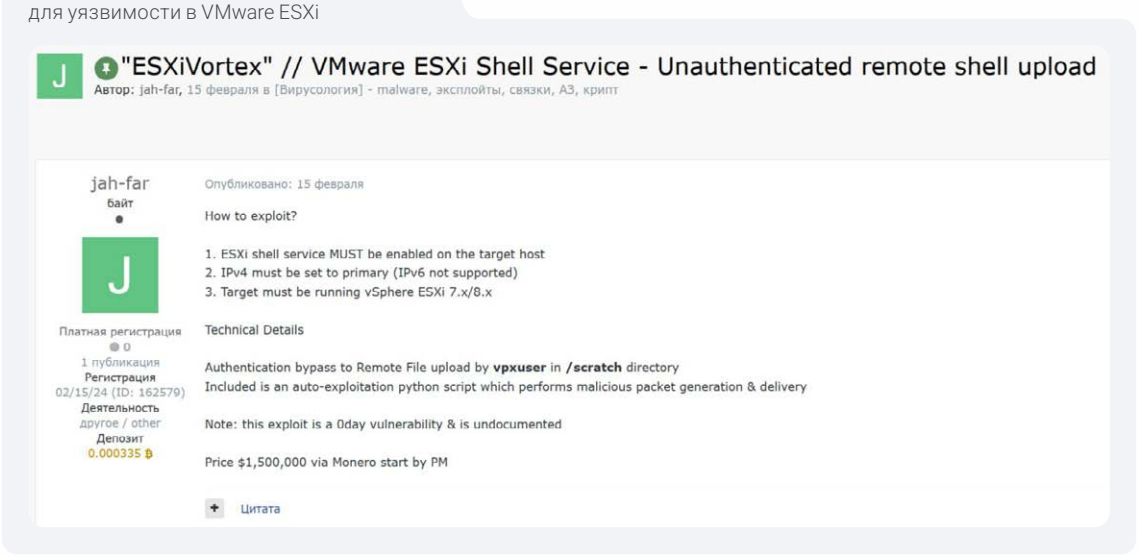
Объявление о продаже эксплоита для уязвимости в межсетевом экране Palo Alto

Подобные публично доступные приложения пользуются большой популярностью у киберпреступников, в том числе тех, которые занимаются шпионажем. Продавец подчеркивает, что сейчас доступно более 14 000 уязвимых устройств, и обещает предоставить видео с доказательством работоспособности эксплоита.

VMware ESXi

Продавец предлагает эксплоит для уязвимости в VMware ESXi — еще одном программном обеспечении, популярном среди злоумышленников, которые распространяют программы-вымогатели.

Объявление о продаже эксплоита для уязвимости в VMware ESXi



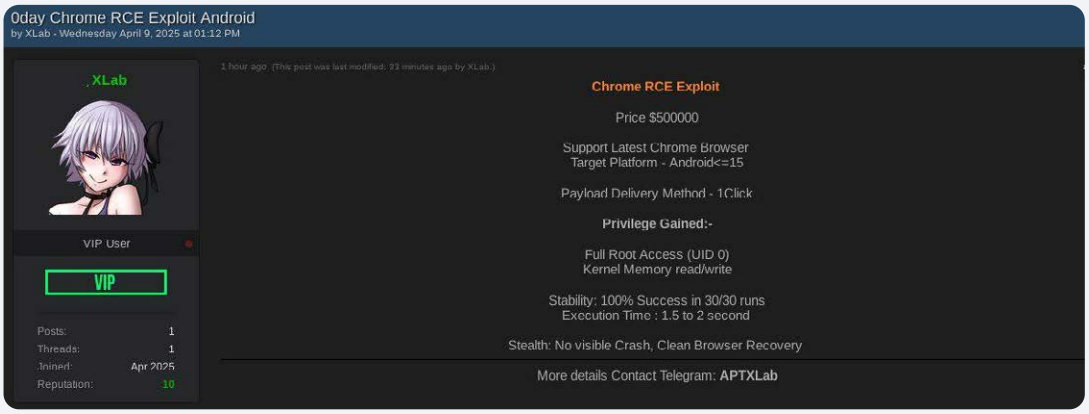
По заявлению автора, эксплоит позволяет загрузить вредоносный файл в папку `/scratch` от имени `vpxuser`. Такая функция может использоваться для обнаружения подозрительной активности или ее проактивного поиска.

Ввиду популярности и критичности VMware ESXi продавец просит за эксплоит $ 1 500 000 в криптовалюте Monero.

Браузер Google Chrome

На теневых ресурсах можно найти объявления о продаже эксплоитов для уязвимостей не только в приложениях для Windows, но и в ПО для мобильных устройств, например Android.

Объявление о продаже эксплоита для уязвимости в браузере Google Chrome

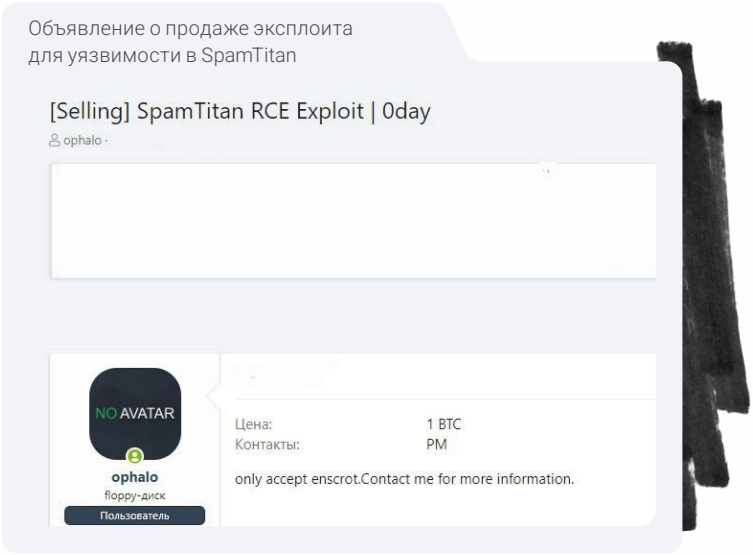


В этом объявлении автор предлагает 0-day-эксплоит для уязвимости, которая позволяет выполнить вредоносный код на устройстве, в браузере Chrome. Продавец утверждает, что эксплоит работает на всех версиях Android до 15.

Антиспам-решение SpamTitan

Некоторые объявления содержат минимум информации. Например, в этом автор предлагает написать ему личное сообщение, чтобы узнать детали.

Объявление о продаже эксплоита для уязвимости в SpamTitan

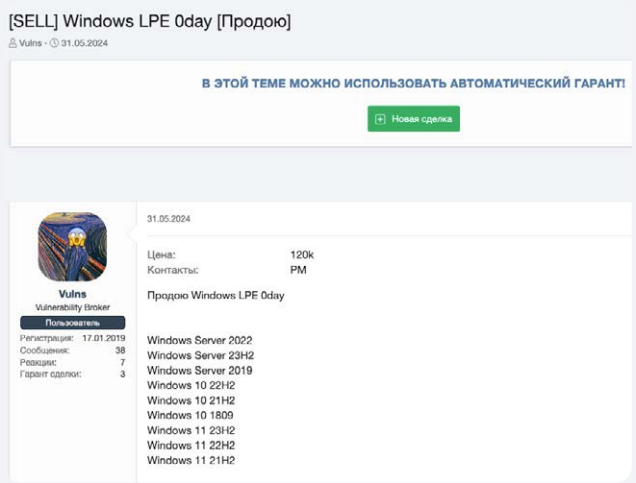


Продавец предлагает 0-day-эксплоит для уязвимости, которая позволяет удаленно выполнить вредоносный код в антиспам-решении SpamTitan. Как и в ранее описанном случае с межсетевым экраном, в этой ситуации злоумышленник может начать атаку с компрометации средства обеспечения кибербезопасности.

Повышение привилегий в Windows

Злоумышленникам зачастую нужно не только получить первоначальный доступ к той или иной системе, но и повысить имеющиеся привилегии, чтобы, например, продвинуться дальше по скомпрометированной IT-инфраструктуре. На теневых ресурсах встречаются объявления о 0-day-эксплоитах для уязвимостей, позволяющих решить эту задачу.

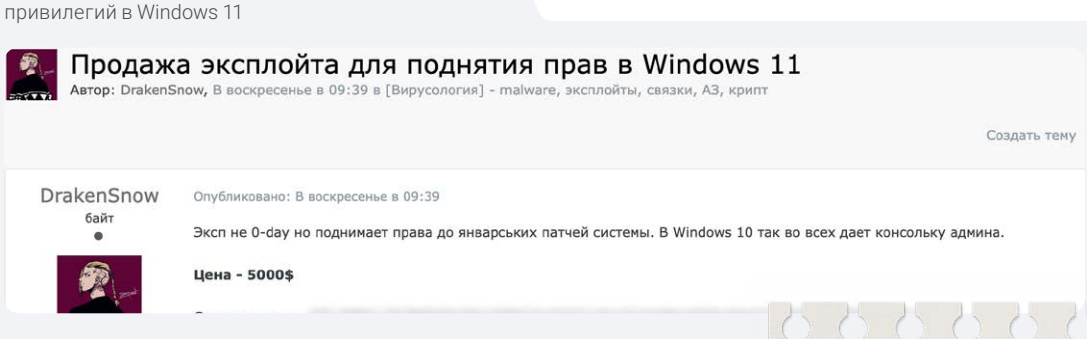
Объявление о продаже эксплоита для повышения привилегий в Windows



В объявлении выше автор предлагает 0-day-эксплоит для уязвимости во многих версиях Windows, которая позволяет повысить привилегии в скомпрометированной системе.

Продавец просит за эксплоит $ 120 000

Объявление о продаже эксплоита для повышения привилегий в Windows 11



Еще один пример похожего объявления. В этот раз продавец фокусируется на том, что его эксплоит позволяет повысить привилегии в наиболее актуальных версиях Windows.

При этом цена намного ниже, чем в предыдущем варианте, — всего $ 5 000

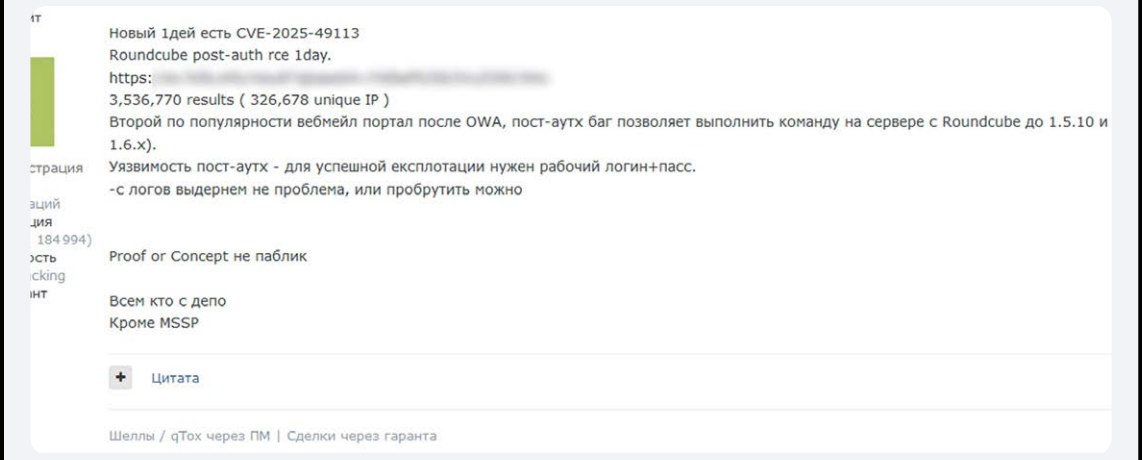
Объявления о продаже эксплоитов для известных уязвимостей

На теневых ресурсах злоумышленники также активно предлагают эксплоиты к уже известным уязвимостям. Обычно таким ВПО легко воспользоваться: его стоимость ниже, чем у эксплоитов для 0-day-уязвимостей, а продавцы предлагают поддержку. Поэтому среди атакующих этот сегмент теневого рынка довольно популярен. Рассмотрим несколько примеров подобных объявлений.

Roundcube

Автор предлагает эксплоит для уязвимости с идентификатором CVE-2025-49113 в Roundcube.

Объявление о продаже эксплоита для уязвимости с идентификатором CVE-2025-49113 в Roundcube



Для успешной эксплуатации покупателю понадобятся актуальные учетные данные жертвы. И автор ВПО готов их предоставить: он планирует получить их из логов стилеров или путем перебора паролей.

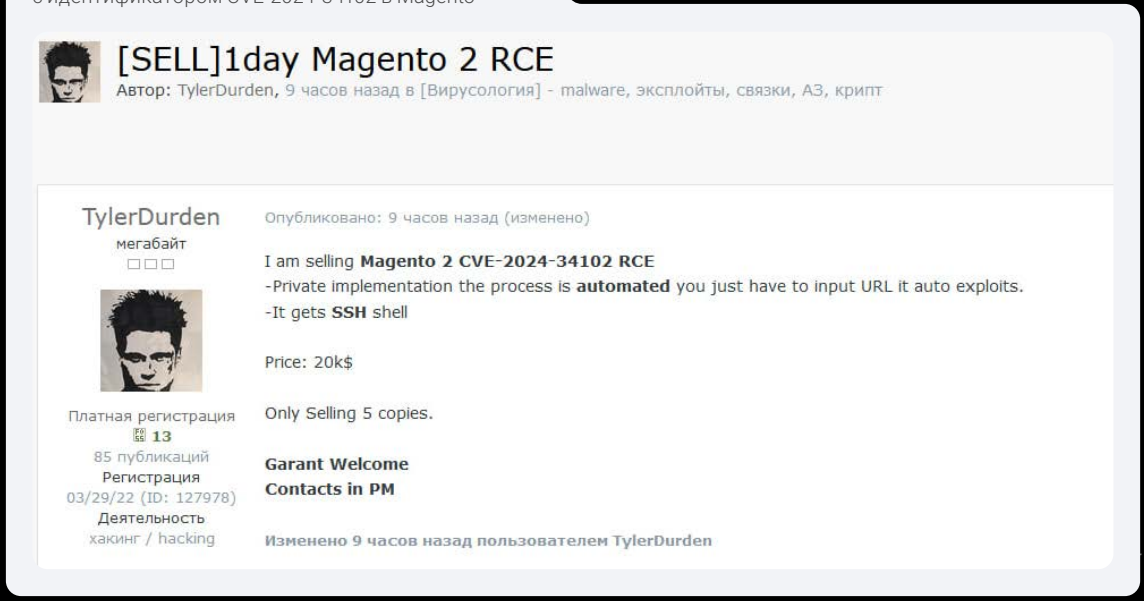
Доступ к веб-приложениям

На теневых ресурсах встречаются предложения об эксплоитах, которые позволяют получить доступ к веб-приложению, чтобы разместить там ВПО для последующей загрузки, получить доступ к персональным данным или для других атак.

Объявление о продаже эксплоита для уязвимости с идентификатором CVE-2024-10924

В этом объявлении автор предлагает эксплоит для уязвимости с идентификатором CVE-2024-10924 в плагине Really Simple Security для WordPress. Успешная эксплуатация позволит злоумышленнику получить полный доступ к веб-приложению.

Объявление о продаже эксплоита для уязвимости с идентификатором CVE-2024-34102 в Magento

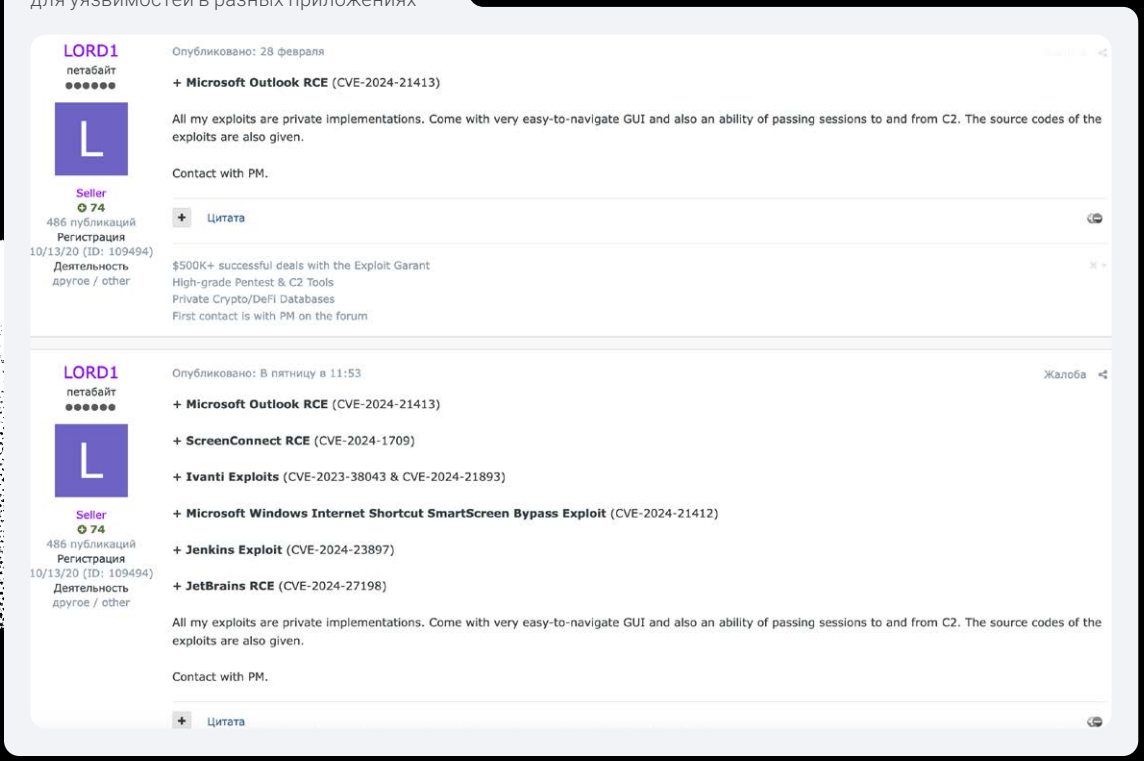


Еще один похожий пример — объявление о продаже эксплоита для уязвимости с идентификатором CVE-2024-34102 в Magento. По заверению продавца, эксплуатация полностью автоматизирована. Все, что требуется от злоумышленника, — предоставить URL сайта. В результате атакующий получит доступ по SSH. Автор предупреждает, что готов продать только пять копий инструмента.

Набор эксплоитов

На теневых ресурсах встречаются объявления, в которых не только продают набор эксплоитов для уязвимостей в самых разных приложениях, но и предлагают регулярно обновлять его.

Объявление о продаже эксплоитов для уязвимостей в разных приложениях

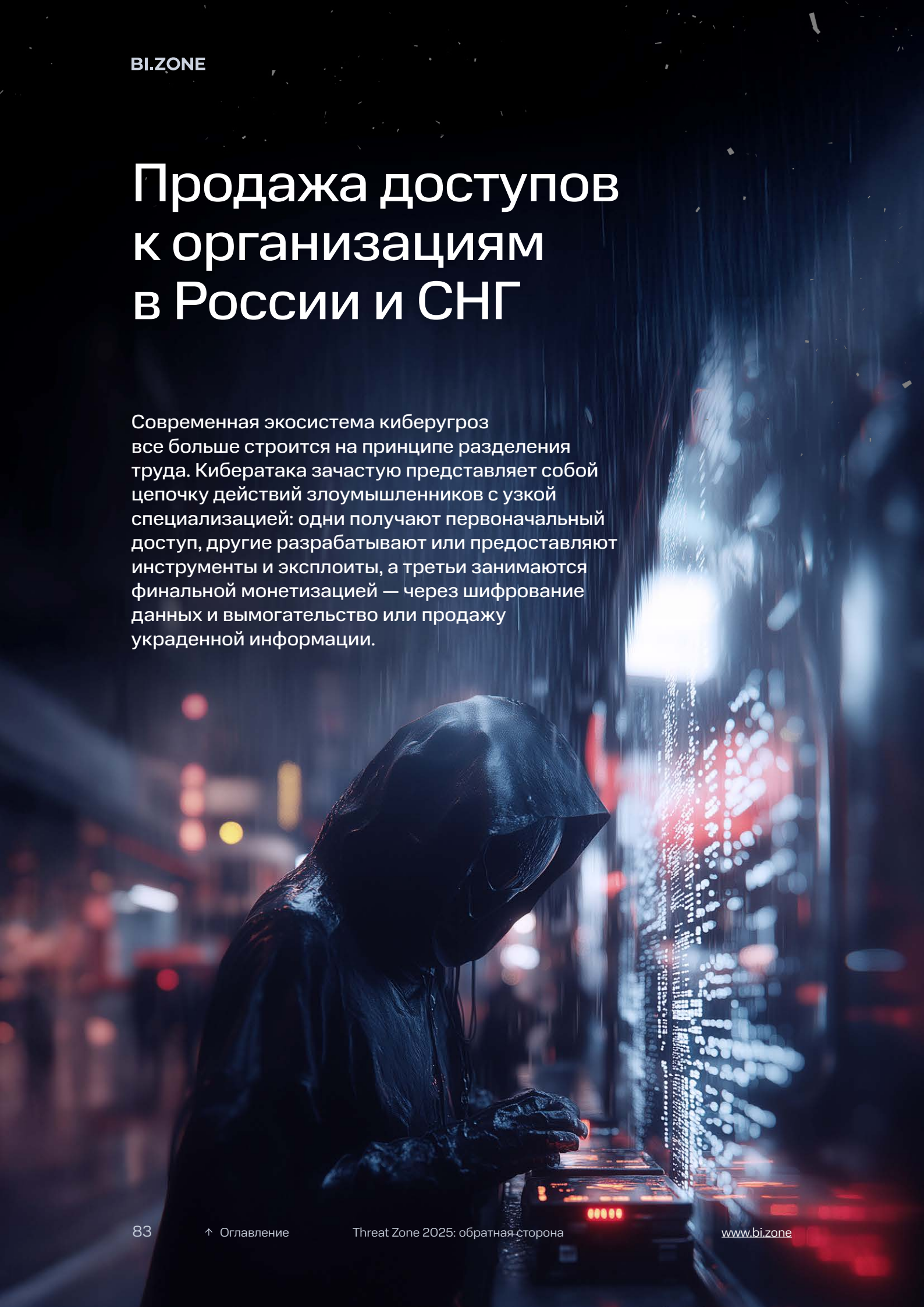


Автор отмечает, что готов предоставить исходные коды своего ВПО, а для удобной работы доступен графический пользовательский интерфейс (graphical user interface, GUI). Еще утверждает, что провел успешные сделки более чем на 500 000 $ и все эксплоиты — его личная разработка.

Чтобы построить эффективную киберзащиту организации, важно знать, какие уязвимости эксплуатируют злоумышленники в реальных атаках. Поэтому мы рекомендуем использовать данные портала BI.ZONE Threat Intelligence. Он предоставляет подробную информацию о таких уязвимостях и дает возможность корректно приоритизировать их исправление.

Продажа доступов к организациям в России и СНГ

Современная экосистема киберугроз все больше строится на принципе разделения труда. Кибератака зачастую представляет собой цепочку действий злоумышленников с узкой специализацией: одни получают первоначальный доступ, другие разрабатывают или предоставляют инструменты и эксплоиты, а третьи занимаются финальной монетизацией — через шифрование данных и вымогательство или продажу украденной информации.



В этой системе важной фигурой выступает брокер первоначального доступа (initial access broker, IAB). Это злоумышленник или группа, которые специализируются на проникновении во внутренние сети организаций и перепродаже доступа другим участникам киберпреступной экосистемы. Брокеры не занимаются вымогательством или шифрованием, их задача — собрать активы: взломанные VPN, RDP, уязвимые веб-панели, доступы к корпоративным почтовым системам и т. д.

На теневых форумах регулярно публикуют предложения о продаже доступа к корпоративным сетям. Примерно в 70% объявлений речь идет о привилегированном доступе. Хотя основной спрос приходится на организации из Западной Европы и Северной Америки, активно предлагают и доступы к компаниям из России и стран СНГ. Примечательно, что на фоне роста числа хактивистских атак в России стали чаще бесплатно распространять доступы к корпоративным сетям в теневых чатах и на форумах.

В четвертой части исследования мы рассмотрим примеры объявлений о продаже доступов к корпоративным сетям в России и странах СНГ. Также приведем данные о стоимости разных типов доступов.

Типы доступов

Собрали основные типы доступов, которые встречаются в объявлениях на теневых ресурсах.

VPN-доступ

Учетные данные для подключения к корпоративной VPN.

от $ 500

RDP (Remote Desktop Protocol)

Доступ к удаленному рабочему столу сотрудника или серверу.

от $ 1000

В зависимости от уровня привилегий и компании.

Аккаунты для доступа к корпоративной сети

Различные учетные записи для входа в корпоративные системы (необязательно с высокими правами).

от $ 10

За базовые аккаунты.

OWA (Outlook Web Access)

Доступ к корпоративной почте через веб-интерфейс.

от $ 100

Факторы, влияющие на стоимость доступов

Размер и доходы компании-жертвы

Чем крупнее бизнес и выше его обороты, тем дороже доступ.

Сфера деятельности

Доступы к финансовым, промышленным, телекоммуникационным и IT-компаниям традиционно оцениваются выше.

Уровень привилегий

Доступ администратора и доступ к критически важным ресурсам ценятся выше, чем стандартные УЗ.

Эксклюзивность

Если продавец гарантирует уникальность доступа — то есть продает его одному покупателю — цена увеличивается.

Наличие дополнительных данных

Если в комплекте идут базы данных, email-адреса, внутренние документы и другая информация, стоимость повышается.

Потенциал для дальнейшей монетизации

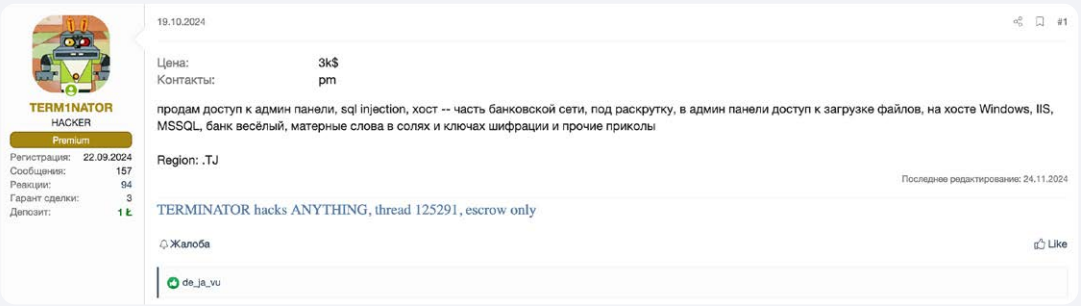
Если доступ можно использовать для вымогательства, кражи данных или шпионажа, его цена возрастает.

Примеры объявлений о продаже доступов

Доступ к административной панели банка Таджикистана

Пользователь теневого форума TERM1NATOR предложил купить несанкционированный доступ к административной панели хоста, являющегося частью инфраструктуры банка в Таджикистане.

Объявление о продаже доступа к инфраструктуре банка



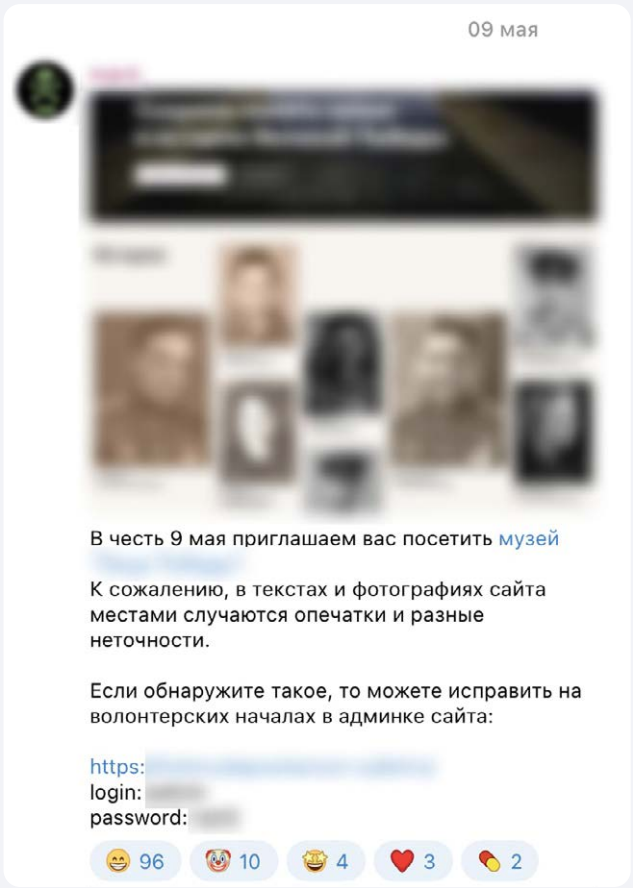
Судя по описанию, доступ получен через SQL-инъекцию и позволяет загружать файлы. Потенциально это может привести к удаленному выполнению команд и развертыванию вредоносного ПО. Хост работает на Windows Server с IIS и MS SQL. Относительно низкая стоимость базы — возможный признак срочной продажи.

Раздел «Теневые ресурсы» на портале BI.ZONE Threat Intelligence поможет отследить информацию о продаже первоначальных доступов к скомпрометированным организациям. Это позволит не допустить дальнейшего продвижения злоумышленников в инфраструктуре.

Доступ к административной панели музейного сайта

В годовщину Дня Победы в телеграм-канале хактивистской направленности опубликовали данные для входа в административную панель сайта одного из проектов, посвященных истории Великой Отечественной войны.

Объявление в телеграм-канале злоумышленников с призывом «исправлять опечатки» на сайте музея



Сообщение имитирует призыв к волонтерам помочь с редактированием исторических данных. Однако авторство канала свидетельствует о приглашении к несанкционированному изменению сведений.

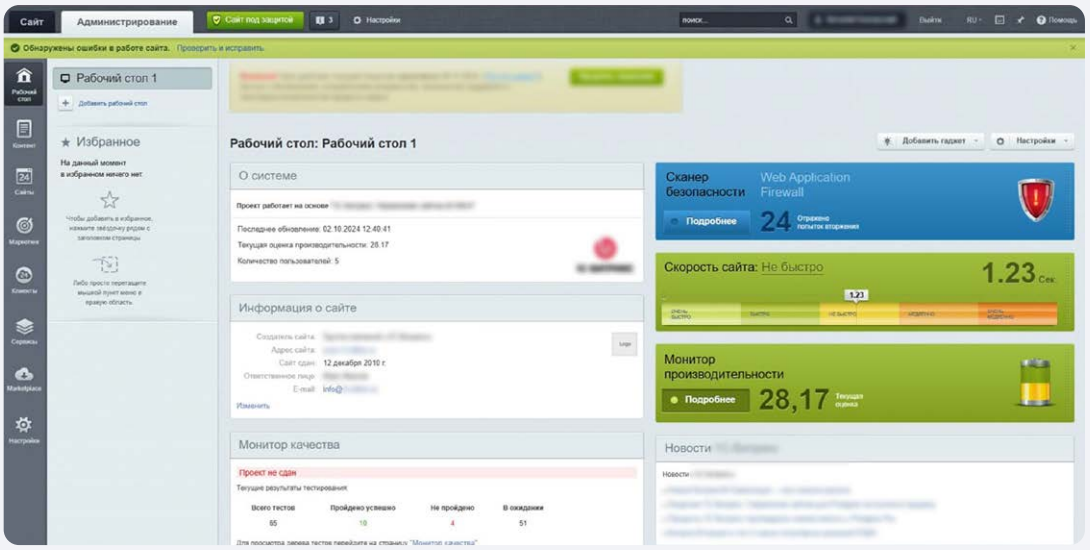
Компрометация подобного ресурса не дает финансовой выгоды, однако для хактивистов главный мотив — получить широкий резонанс. Поэтому целью атаки выбрали проект на чувствительную тему.

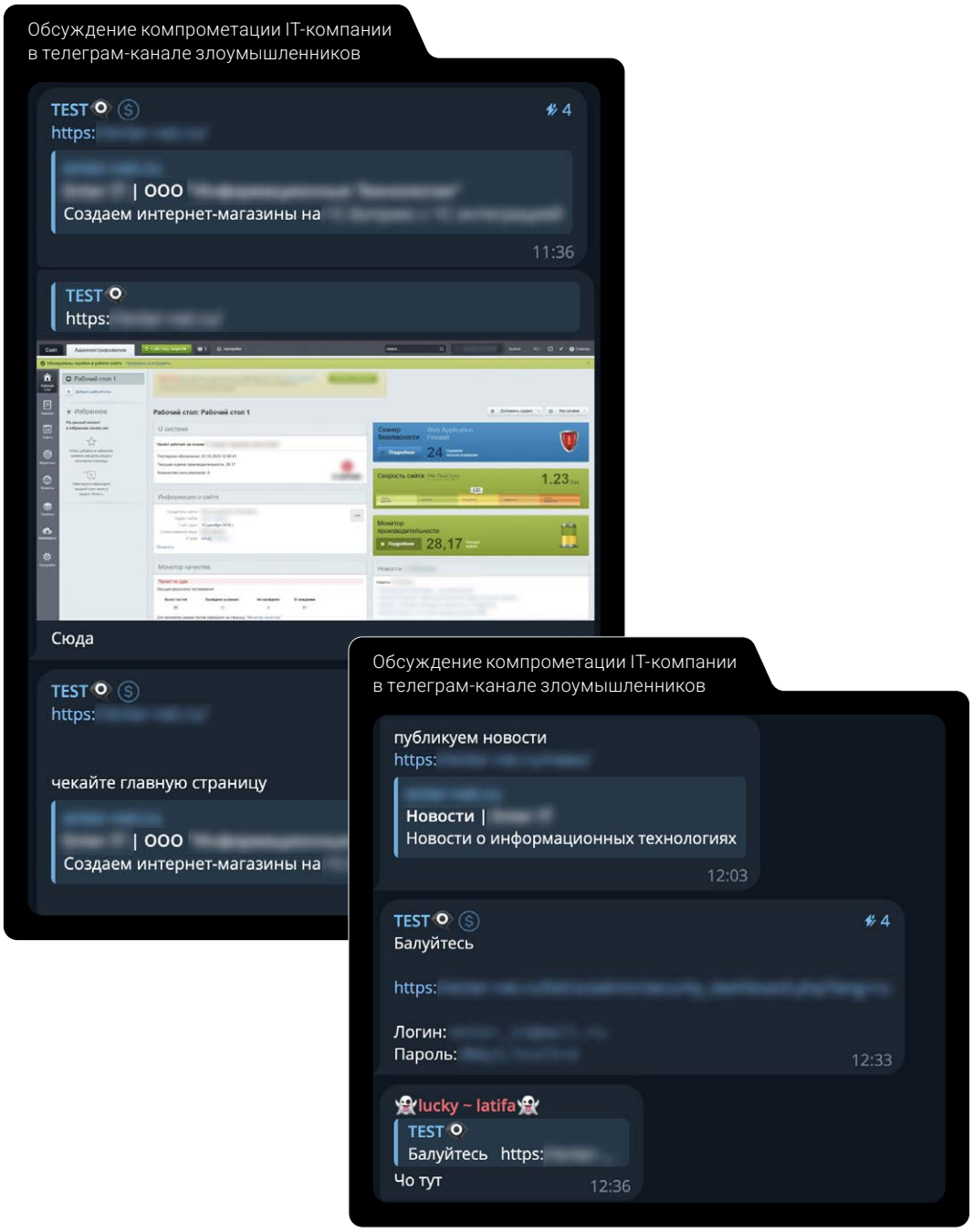
Доступ к админ-панели сайта IT-компании

Злоумышленники выложили в телеграм-чат учетные данные и ссылки на внутренние разделы CRM-системы IT-компании, занимающейся разработкой сайтов и сопровождением инфраструктуры.

В подтверждение своих действий они также опубликовали скриншоты интерфейса административной панели.

Скриншот админ-панели скомпрометированной IT-компании





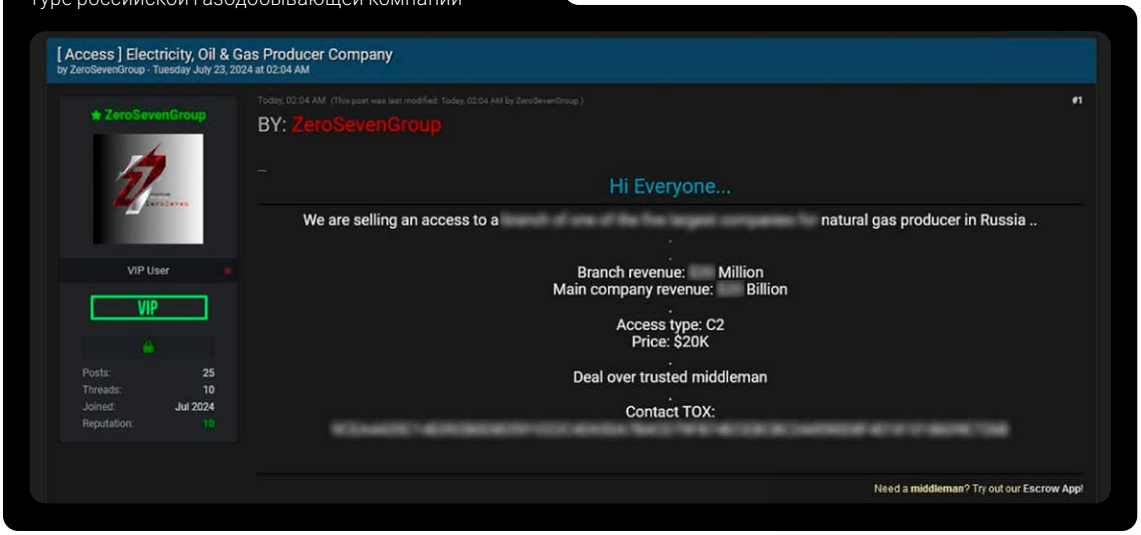
Из обсуждения в чате следует, что через инфраструктуру этой компании был скомпрометирован клиент — оптовый производитель женской одежды, чей сайт находился на техническом обслуживании.

Этот инцидент демонстрирует типичный вектор атаки через подрядчика, когда компрометация сервисной организации приводит к получению вторичного доступа к системам ее клиентов.

Доступ к инфраструктуре газодобывающей компании

Объявления о продаже доступов к рабочим станциям или серверам внутри корпоративных сетей пользуются спросом на теневых форумах. Особенно когда речь идет об организациях из критически важных отраслей. Например, на одном из теневых форумов пользователь ZeroSevenGroup предложил доступ к инфраструктуре филиала одной из газодобывающих компаний России.

Объявление с предложением доступа к инфраструктуре российской газодобывающей компании



Доступ предоставляется в формате C2 (Command and Control). Это свидетельствует об уже состоявшемся проникновении в инфраструктуру. Кроме того, злоумышленники заявляют о возможности подключения через RDP, SSH или VPN.

Сумма сделки — $ 20 000

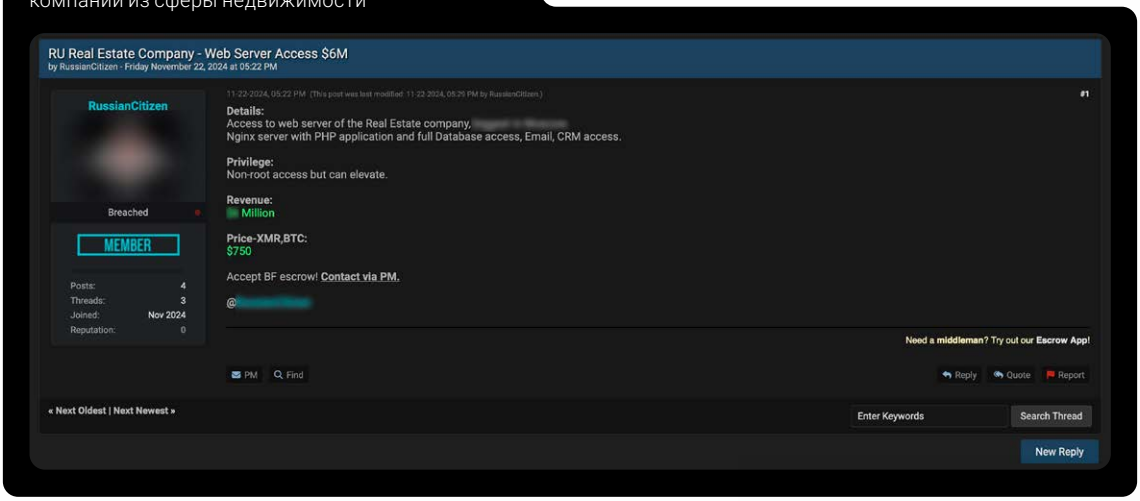
Указание крупной суммы сделки (20 000 $) и упоминание масштаба компании (доход в миллиардах долларов) — типичная практика для подобных предложений. В этом случае цена определяется не уровнем доступа как таковым, а потенциальной ценностью инфраструктуры для заинтересованных сторон.

Этот пример иллюстрирует распространенную схему: после успешного проникновения в сеть атакующие создают устойчивый канал управления, оценивают потенциал инфраструктуры и выставляют доступ на продажу.

Доступ к веб-серверу компании из сферы недвижимости

На теневом форуме разместили предложение о продаже доступа к веб-серверу крупной московской компании в сфере недвижимости. По заявлению продавца, годовой доход организации исчисляется миллионами долларов. Это подчеркивает значимость компании, а также ценность информации, которую можно получить после покупки доступов.

Объявление о продаже доступа к веб-серверу компании из сферы недвижимости



Злоумышленник предлагает доступ к серверу, работающему на nginx с PHP-приложением. В объявлении также указано наличие полного доступа к базе данных, электронной почте и CRM-системе компании. Хотя текущий уровень доступа не root, продавец утверждает, что возможна эскалация привилегий.

Стоимость доступа — $750

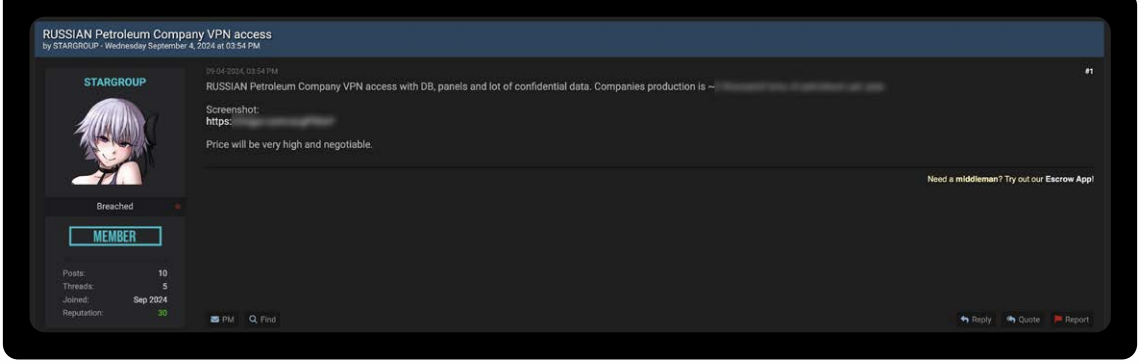
Оплата принимается в криптовалюте (XMR и BTC).

Вероятно, злоумышленник воспользовался уязвимостью в PHP-приложении или неправильной конфигурацией связки nginx + PHP-FPM. Это распространенный вектор атаки, который часто позволяет получить возможность удаленного выполнения кода (RCE) на сервере.

Доступ к VPN нефтедобывающей компании

Следующее объявление содержит информацию о продаже доступа к VPN российской нефтяной компании. Согласно описанию, доступ позволяет подключаться к корпоративной инфраструктуре и взаимодействовать с базами данных, административными интерфейсами и внутренней документацией.

Объявление о продаже доступов к VPN нефтедобывающей компании



Важно отметить, что речь идет не о простом техническом туннеле, а о полноценном доступе к внутренним ресурсам через валидные учетные данные с расширенными правами. Это значительно повышает ценность предложения и одновременно увеличивает потенциальные риски для компании-жертвы: при таком уровне доступа возможны масштабные утечки информации, акты саботажа или вымогательство.

Вероятнее всего, действующие УЗ были получены с помощью стилеров или из ранее скомпрометированных источников. Такой подход существенно снижает вероятность быстрого обнаружения и позволяет злоумышленникам дольше оставаться в сети незамеченными.

В качестве доказательства масштабов организации продавец приложил скриншот с производственными показателями, где указан объем добычи.

На высокую значимость и востребованность доступа указывает тот факт, что стоимость не указана. Это может говорить о намерении вести индивидуальные переговоры или сначала оценить рыночный спрос.

Сообщения о компрометации организаций

Мы изучили объявления об утечках данных, которые были опубликованы на теневых ресурсах в 2024-м и первой половине 2025 года. Основное внимание уделили тому, какого типа данные попадают в открытый доступ, где размещаются сообщения об утечках и как меняются каналы распространения.

Площадки для публикации

В основном украденные данные распространяются через:

Telegram

Благодаря анонимности, высокой скорости и простоте использования эта платформа продолжает оставаться ключевым инструментом как для киберпреступников, так и для их аудитории.

Закрытые даркнет-форумы

По-прежнему используются для «тяжелых» сливов финансовой информации, баз с персональными данными, корпоративными документами.

Статистика сообщений об утечках
в 2024 году — первой половине 2025 года:

568
сообщений
разместили в Telegram

362
объявления появилось
на даркнет-форумах

Большее количество сообщений в Telegram показывает, что активность злоумышленников смещается в сторону более открытых и быстро реагирующих площадок. Особенно это заметно в русскоязычном сегменте интернета, где Telegram становится своего рода маркетплейсом для слива информации.

Содержание объявлений

Анализ объявлений об утечках показывает, что состав публикуемой информации в целом остается неизменным. Чаще всего в утечках фигурируют:

- **Логины и пароли.** В том числе скомпрометированные аутентификационные данные от корпоративных и личных аккаунтов.
- **Телефоны.** Особенно часто в утечках, связанных с сервисами доставки, банками, онлайн-магазинами.
- **Email.** При этом почта привязана к конкретным пользователям или сотрудникам компаний.

Однако на этом фоне в 2025 году четко прослеживается новая тенденция: растет доля объявлений об утечках внутренней документации компаний. Раньше утечки такой информации были редкими, но теперь встречаются все чаще. Среди документов:

- Финансовая отчетность — бюджеты, балансы, инвестиционные планы.
- Юридические документы — договоры с клиентами и подрядчиками, претензии, судебные иски.
- Служебные записки и переписка — включая внутренние чаты, электронную почту и отчеты о совещаниях.
- Материалы по кибербезопасности — регламенты, инструкции, отчеты о внутренних проверках, инцидентах и даже расследованиях.

Это свидетельствует о двух важных изменениях:

- Атакующие получают более глубокий доступ. Теперь они проникают не только в пользовательские базы, но и в инфраструктуру компаний, а также перехватывают внутренний документооборот.
- Растет спрос на коммерчески значимую информацию. Она интересует не только конкурентов, но и недобросовестных сотрудников, а также киберпреступников.

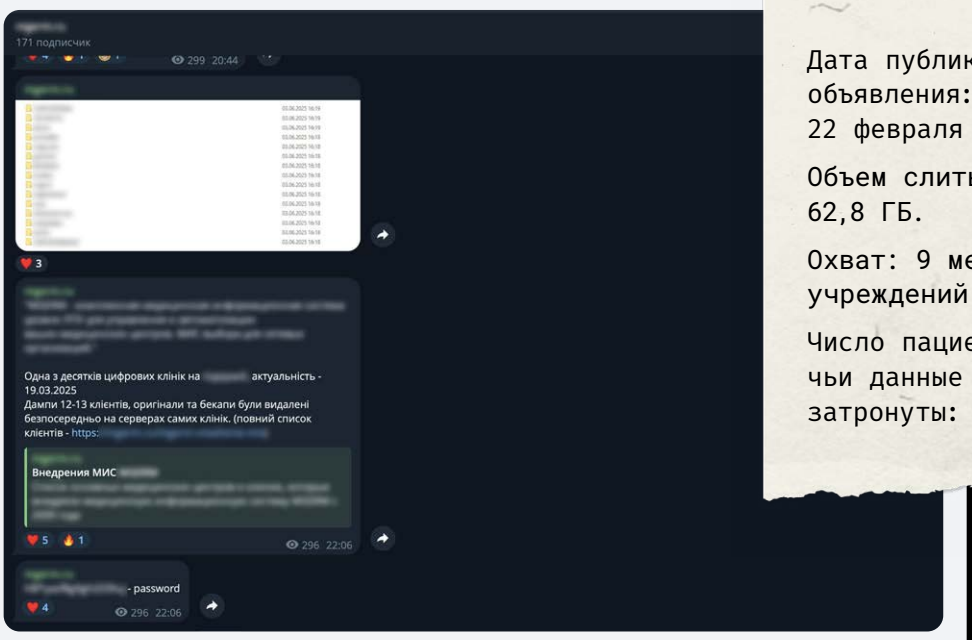
Все это увеличивает риски репутационных, юридических и финансовых потерь для организаций — особенно в условиях, когда утечки становятся публичными и активно распространяются.

Примеры объявлений об утечках

Компания — разработчик медицинской информационной системы

Один из инцидентов 2025 года связан с компанией — разработчиком платформы, которая предназначена для автоматизации процессов в клиниках, стационарах, санаториях и НИИ.

Сообщение злоумышленников о взломе компании — разработчика платформы для медицинской сферы



Дата публикации объявления:
22 февраля 2025 г.

Объем слитых данных:
62,8 ГБ.

Охват: 9 медицинских учреждений.

Число пациентов, чьи данные были затронуты: более 32 000.

Содержание утечки

Киберпреступники заявили, что открывают доступ к амбулаторным картам пациентов с конфиденциальной медицинской и персональной информацией:

- Ф. И. О.,
- дата рождения,
- должность,
- email,
- телефон,
- паспортные данные,
- номер социальной карты,
- информация о ДМС,
- адрес регистрации,
- диагнозы,
- данные пенсионного удостоверения.

Особенности инцидента

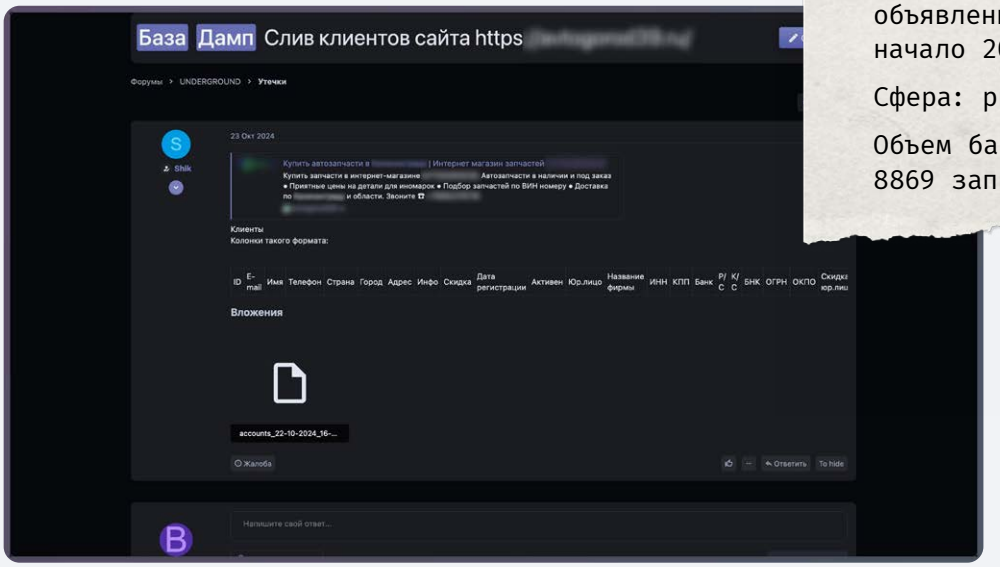
Утечка содержала чувствительные медицинские данные, которые в соответствии с законодательством (в том числе с 152-ФЗ и HIPAA, если речь идет о международном обмене) подлежат особой защите.

Киберпреступники заявили, что получили доступ напрямую к внутренней инфраструктуре системы. Подобные инциденты не только создают риски для пациентов, но и подрывают доверие к медицинским учреждениям и цифровым системам в целом.

Интернет-магазин автозапчастей

В открытом доступе появилась база данных интернет-магазина — регионального ритейлера автозапчастей.

Сообщение злоумышленников, в котором предлагается база данных интернет-магазина



Дата публикации объявления: начало 2025 г.

Сфера: ритейл.

Объем базы: 8869 записей.

Содержание утечки

- Ф. И. О.
- Email.
- Адрес доставки.
- ИНН — как частных лиц, так и, вероятно, организаций или ИП.

Особенности инцидента

Хотя объем утечки сравнительно невелик, в нее попали персональные данные, защита которых регулируется 152-ФЗ.

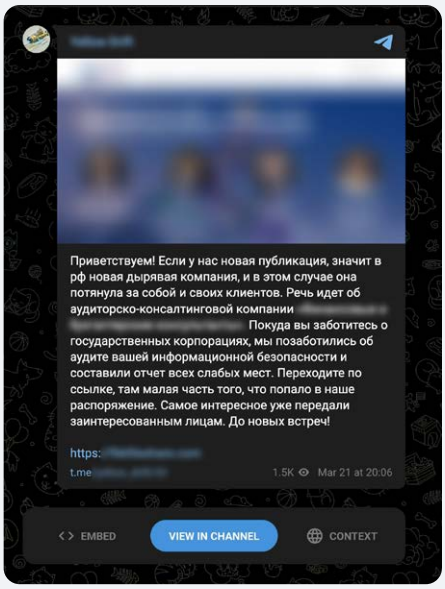
Наибольшую ценность для злоумышленников представляют адреса и ИНН. Эти сведения могут использоваться для целевого фишинга или оформления мошеннических договоров.

Этот случай показывает: даже небольшие региональные интернет-магазины становятся объектом внимания киберпреступников, особенно если пренебрегают базовыми мерами кибербезопасности. Также он подтверждает, насколько важна защита персональных данных не только для крупных компаний, но и для малого бизнеса. Утечка даже нескольких тысяч записей способна повлечь серьезные последствия — от штрафов до потери доверия со стороны клиентов.

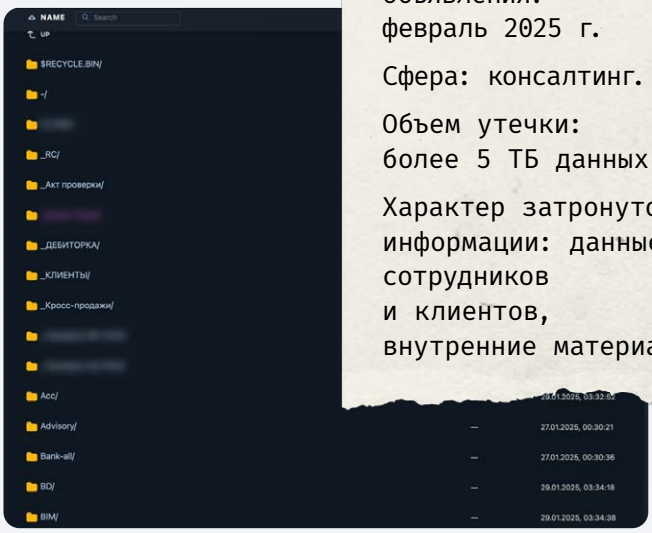
Аудиторско-консалтинговая компания

Одна из крупнейших утечек 2025 года затронула аудиторско-консалтинговую компанию — структуру, работающую с корпоративной, налоговой и персональной информацией большого количества клиентов. Ответственность за атаку взяла на себя кибергруппировка Yellow Drift.

Объявление о взломе компании в телеграм-канале злоумышленников



Папки с похищенными данными на сайте злоумышленников



Дата публикации объявления: февраль 2025 г.

Сфера: консалтинг.

Объем утечки: более 5 ТБ данных.

Характер затронутой информации: данные сотрудников и клиентов, внутренние материалы.

Содержание утечки

- Персональные данные сотрудников (в том числе паспортные данные, контакты, ИНН, СНИЛС).
- Информация о клиентах компании — договоры, финансовая отчетность.
- Материалы внутренних проектов и служебная переписка.
- Скан-копии документов — удостоверений личности, доверенностей, подписей.
- Фотографии с корпоративных мероприятий.
- Документы по налоговому учету.

Особенности инцидента

Утечка затронула персональные и конфиденциальные коммерческие данные, создав для десятков клиентов компании комплексные риски — репутационные, юридические и операционные.

Из-за объема скомпрометированных данных — несколько терабайтов — утечка стала одной из крупнейших в российском сегменте за последние годы.

Наличие в утекших данных договорной документации и информации о внутренних проектах открыло возможности для экономического шпионажа, мошенничества и давления на клиентов.

Этот инцидент — тревожный сигнал для всех организаций, работающих с чувствительными данными. Даже крупные консалтинговые компании с формально выстроенными системами защиты могут оказаться уязвимыми перед целевыми атаками.

Микрофинансовая компания

В открытом доступе была обнаружена база данных, принадлежащая микрофинансовой компании из сферы автозалогового кредитования.

Содержание утечки

- Ф. И. О.
- Дата рождения.
- Адрес регистрации.
- Паспортные данные (серия, номер, дата выдачи, орган, выдавший документ).
- Телефон.
- Email.

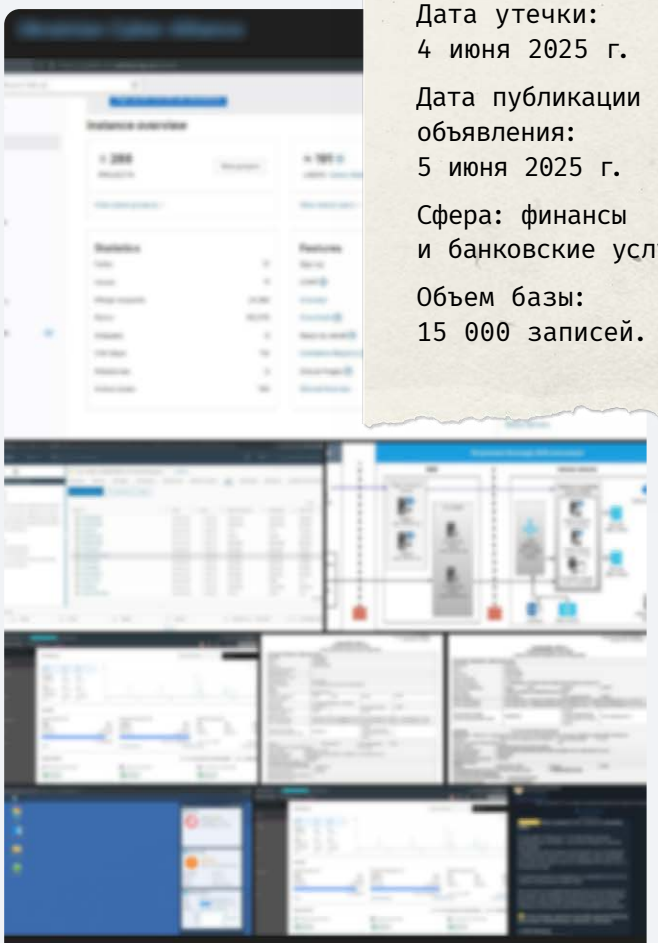
Особенности инцидента

Данные появились в открытом доступе практически сразу после утечки. Она включала полный комплект персональных данных, достаточный для мошеннических операций, включая оформление займов и сим-карт.

Особую опасность представляет сфера деятельности компании (микрофинансирование), так как это создает риски вторичного использования данных — для шантажа, фишинга или подачи фальшивых заявок на кредиты.

Этот случай наглядно показывает, насколько важен постоянный мониторинг утечек для финансовых организаций. Компрометация даже небольших по объему баз данных может привести к серьезным финансовым потерям клиентов и ущербу для репутации компаний.

Сообщение о взломе сайта микрофинансовой компании



[redacted] hacked the company [redacted], which issues secured loans. The company is linked to the [redacted]
The infrastructure (hundreds of virtual machines and hundreds of terabytes of data) has been completely destroyed

As a result, we obtained data on a large number of borrowers, including various [redacted], as well as [redacted], for example, data of employees from the [redacted] (known for its cyberattacks under the names [redacted])

The company partially acknowledged the hack, stating that "the security system triggered and they shut down the old website." We did. Along with the phones and all the infrastructure. So, the old loan shark should be investigated by regulators — [redacted] and [redacted]

Дата утечки:
4 июня 2025 г.

Дата публикации объявления:
5 июня 2025 г.

Сфера: финансы и банковские услуги.

Объем базы:
15 000 записей.

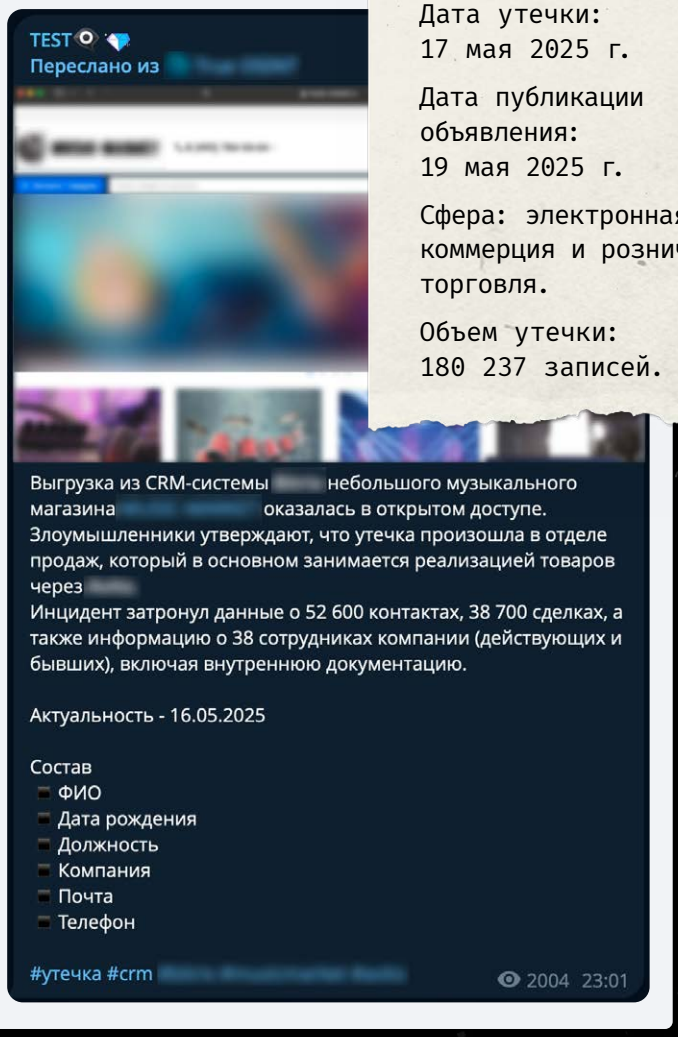
Интернет-магазин музыкальных инструментов

В открытом доступе появилась обширная база данных, принадлежащая интернет-магазину музыкальных инструментов.

Содержание утечки

- Ф. И. О.
- Email.
- Телефон.
- Дата рождения.
- Информация о месте работы (компания, должность, подразделение).
- Ссылки на соцсети и мессенджеры (Facebook*, Telegram, «ВКонтакте», Skype, личная страница).

Сообщение об утечке с сайта музыкального интернет-магазина



Дата утечки:
17 мая 2025 г.

Дата публикации объявления:
19 мая 2025 г.

Сфера: электронная коммерция и розничная торговля.

Объем утечки:
180 237 записей.

Особенности инцидента

Утечка выделяется не только масштабом, но и глубиной раскрытия профилей каждого пользователя. В зоне риска оказались:

- персональные данные;
- сведения о профессии и должности;
- цифровой социальный след (привязка к мессенджерам и соцсетям).

Инцидент иллюстрирует новый тренд: злоумышленники все чаще стремятся не просто быстро заработать через доступ к аккаунтам, а получают более чувствительные и стратегически ценные данные. Утечки подобных данных особенно опасны для компаний, потому что их можно использовать:

- для фишинга и других методов социальной инженерии;
- шантажа и давления на бизнес;
- конкурентной разведки (если среди пострадавших — сотрудники B2B-компаний);
- дестабилизации бизнес-процессов.

На этом фоне защита клиентских данных перестает быть задачей исключительно кибербезопасности — теперь это вопрос сохранения репутации бренда.

* Принадлежит компании Meta, которая признана экстремистской организацией и запрещена на территории РФ.

Атакуемые отрасли

Угрозы кибербезопасности распределяются по отраслям неравномерно. Одни сферы становятся объектом внимания злоумышленников значительно чаще других из-за большого объема хранимых данных, высокого уровня цифровизации и множества уязвимостей в инфраструктуре.

Ниже — топ-5 отраслей, наиболее подверженных утечкам данных в 2024–2025 годах.

1. Электронная коммерция и ритейл

Факторы риска:

- объемные пользовательские базы;
- слабая защита личных кабинетов;
- быстрая монетизация данных (карт, логинов, адресов).

Утекают: контакты, адреса доставки, истории покупок, платежные данные.

2. Промышленность и производство

Факторы риска:

- недооцененная роль кибербезопасности в IT-системах;
- использование устаревшего ПО;
- ценные инженерные и проектные данные.

Утекают: внутренние документы, договоры, технические чертежи, переписки с подрядчиками.

3. Общепит и гостиничный бизнес

Факторы риска:

- большой поток клиентов;
- хранение паспортных данных и банковских карт;
- слабая сегментация IT-систем.

Утекают: данные клиентов, сведения о резервациях, платежная информация, отзывы, переписки.

4. Образование

Факторы риска:

- массовое хранение персональных данных студентов и преподавателей;
- низкий уровень защиты в регионах;
- распространенное использование облачных сервисов с уязвимостями.

Утекают: списки учащихся, экзаменационные ведомости, паспорта, данные родителей.

5. Здравоохранение

Факторы риска:

- хранение медицинских и биометрических данных;
- уязвимые информационные системы медицинских учреждений;
- высокая ценность информации для шантажа.

Утекают: амбулаторные карты, диагнозы, истории лечения, данные ДМС, паспортные данные.

Эти отрасли становятся мишенями не только из-за потенциальной прибыли для злоумышленников, но и из-за компрометирующего характера утекающей информации. Утечки таких данных открывают злоумышленникам возможности для давления, шантажа или манипуляции.

Электронная коммерция и ритейл

Поставщик текстильной продукции

Этот случай связан с утекшей базой данных компании, которая занимается поставками текстильной продукции. Утечка затронула значительный объем персональных данных, включая контактную информацию клиентов и партнеров.

Содержание утечки

- Ф. И. О.
- Email.
- Телефон.

Дата публикации объявления:
13 января 2025 г.

Объем утечки:
137 473 записи.

Источник: Telegram.

Особенности инцидента

Несмотря на относительно простой состав утечки (контактные данные без паспортной информации и документов), ее масштаб (более 137 тысяч строк) делает базу ценной для фишинговых и спам-кампаний.

Типичные последствия подобного слива — массовые рассылки, попытки социальной инженерии и ущерб деловой репутации. Кроме того, такие базы часто используются как «сырье» для дальнейшего обогащения через открытые источники.

Интернет-магазин запчастей для бытовой техники

В открытом доступе опубликовали базу данных интернет-магазина, который специализируется на продаже запчастей для бытовой техники. Утечка содержит как контактные, так и технические данные пользователей.

Содержимое утечки

- Логин пользователя.
- Хеш пароля.
- Ф. И. О.
- Телефон.
- Email.
- Почтовый адрес.
- IP-адрес.

Дата утечки и публикации объявления: 10 января 2025 г.

Объем утечки: 64 865 записей.

Источник: Telegram.

Особенности инцидента

Утечка содержит не только персональные и контактные данные, но и хеши паролей, что повышает ее серьезность. Если использовался слабый алгоритм хеширования, злоумышленники могут взломать учетные записи — особенно если пользователи применяли одинаковые пароли на других сайтах.

Наличие IP-адресов также позволяет отслеживать активность и местоположение пользователей, что создает угрозы для приватности и может быть использовано в дальнейших атаках.

Промышленность и производство

Крупный поставщик автосервисного оборудования

В одном из телеграм-каналов выложили базу данных крупного российского поставщика оборудования для автосервисов и СТО.

Содержимое утечки

- Ф. И. О.
- Адрес доставки.
- Телефон.
- Email.

Дата последней записи в БД: 8 ноября 2024 г.

Объем утечки: 764 000 записей о заказах.

Источник: Telegram.

Особенности инцидента

Из-за масштаба эта утечка — одна из крупнейших в сфере B2B-продаж оборудования. Сочетание персональных данных с логистической информацией (адресами доставки) особенно привлекательно для киберпреступников — в первую очередь когда заказчиками выступают юридические лица.

Эти сведения могут использоваться для оформления фальшивых заказов, телефонного мошенничества или подрыва доверия между поставщиком и его клиентами.

Общепит и гостиничный бизнес

Сервис доставки еды

В открытом доступе появилась база данных бургерной, расположенной в одном из городов Подмосковья. Несмотря на относительно небольшой объем утечки, в нее попали чувствительные данные клиентов, включая комментарии к заказам.

Содержимое утечки

- Ф. И. О.
- Email.
- Телефон.
- Адрес.
- Комментарии к заказам.

Дата утечки:
22 апреля 2025 г.

Дата публикации объявления:
25 апреля 2025 г.

Объем утечки:
2695 записей.

Источник:
Telegram.

Особенности инцидента

Даже для малого бизнеса подобные утечки представляют серьезную угрозу. Сочетание контактных данных, адресов доставки и персонализированных комментариев позволяет злоумышленникам легко идентифицировать клиентов. Эти сведения могут использоваться:

- для целевых атак,
- фишинговых рассылок,
- атак с применением других методов социальной инженерии.

Особую опасность представляют комментарии с личными подробностями, например «ребенку», «домофон не работает», «оставить у двери». Этот случай вновь подтверждает необходимость защиты персональных данных в сфере малого и среднего бизнеса.

Туристический портал

В 2025 году в одном из телеграм-каналов появилась база данных крупного агрегатора туристических услуг. Хотя сама утечка произошла давно, ее публикация вновь создала угрозы для пользователей сервиса.

Содержимое утечки

- Ф. И. О.
- Email.
- Телефон.
- IP-адрес.

Дата утечки:
17 августа 2023 г.

Дата публикации объявления:
28 апреля 2025 г.

Объем утечки: 3591 запись.

Источник: Telegram.

Особенности инцидента

Даже устаревшие базы данных представляют ценность для злоумышленников, так как часто содержат постоянные идентификаторы (телефоны, email), которые пользователи применяют в других сервисах. Привязка к IP-адресу может раскрыть географическое местоположение пользователя, а в сочетании с контактными данными — создать основу для фишинга и других методов социальной инженерии.

Этот случай показывает: даже персональные данные, размещенные на государственных или близких к государственным платформах, не всегда надежно защищены.

Образование

Общеобразовательное учреждение

В открытом доступе появилась база данных среднего учебного заведения. Утечка затронула персональные данные учащихся, а также, предположительно, сотрудников. Кроме того, был опубликован доступ к внутренним системам.

Содержимое утечки

- Ф. И. О.
- Логин.
- Хеш пароля.
- Email.
- Telegram.
- Дата рождения.
- Пол.
- Класс.

Дата утечки:
20 января 2025 г.

Дата публикации объявления:
22 января 2025 г.

Объем утечки:
1409 записей.

Источник:
Telegram.

Особенности инцидента

Этот случай — часть серии инцидентов, зафиксированных в 2024 году, когда в открытый доступ попали данные студентов и преподавателей ряда вузов и школ в России и Казахстане. В некоторых случаях среди утекшей информации были логины и пароли от внутренних образовательных систем, что создало реальную угрозу для IT-инфраструктуры учебных заведений.

Чувствительные данные обрабатываются даже на уровне общего образования, при этом сайты учебных заведений зачастую остаются слабо защищенными. Среди возможных рисков — взлом аккаунтов, распространение ВПО через образовательные платформы и вмешательство в учебный процесс.

Частная школа

В другом случае злоумышленники заполучили базу данных частной школы. Утечка содержит высокочувствительную и детализированную информацию, касающуюся учеников и их родителей.

Содержимое утечки

- Ф. И. О.
- Email.
- До трех номеров телефонов.
- Дата рождения.
- Паспортные данные.
- Адрес регистрации.
- Адрес проживания.
- Место работы, рабочие адреса и должности родителей.

Дата утечки: 15 мая 2025 г.

Дата публикации объявления: 16 мая 2025 г.

Объем утечки: 18 490 записей.

Источник: Telegram.

Особенности инцидента

Утечка выделяется высоким уровнем детализации персональных данных. В одном массиве собраны паспортные данные, контакты, информация о местах проживания и о работе родителей. Все это делает базу потенциально опасной как для детей, так и для их семей.

Подобный инцидент чреват не только фишинговыми атаками и мошенничеством, но и реальными физическими угрозами, особенно если злоумышленники сопоставят утекшие данные с геолокацией или активностью в соцсетях.

Этот случай — тревожный прецедент, который вновь подчеркивает необходимость усиленной защиты данных в частных образовательных учреждениях, работающих с социально уязвимой аудиторией.

Здравоохранение

Частная клиника

В открытом доступе появилась база данных крупной частной клиники.

Содержимое утечки

- Ф. И. О.
- Телефон.
- Дата рождения.
- Адрес проживания.

Дата публикации объявления:
27 февраля 2025 г.

Объем утечки:
463 146 записей.

Источник: Telegram.

Особенности инцидента

Хотя официального подтверждения нет, но, по утверждению злоумышленников, утечка включала истории болезней и диагнозы пациентов. Это ставит инцидент в ряд наиболее масштабных утечек медицинских данных за последние годы.

Даже данные из базовых полей — Ф. И. О., даты рождения, адреса и телефоны — позволяют идентифицировать пациентов.

В сочетании с медицинской информацией эти сведения могут быть использованы:

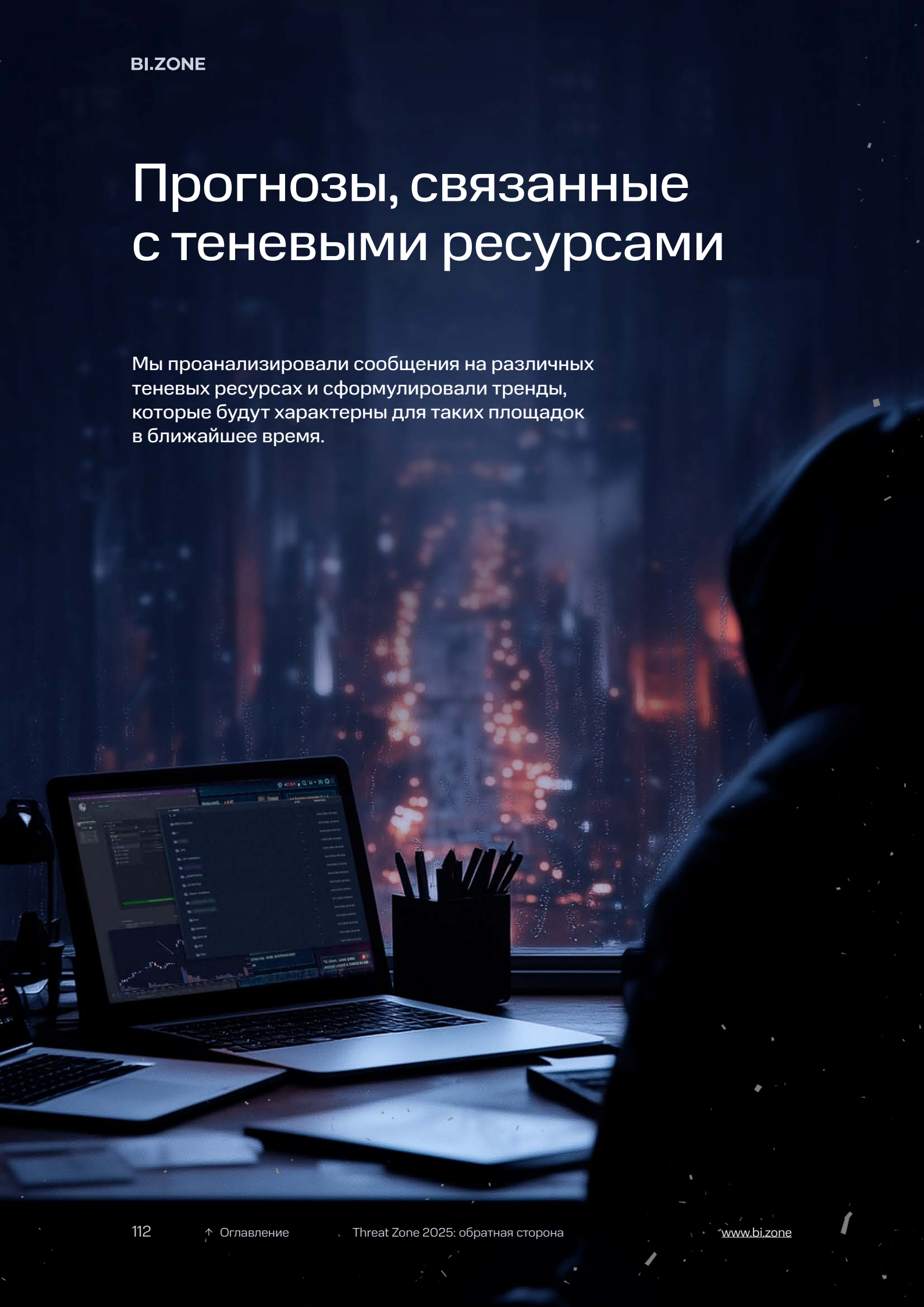
- для шантажа,
- медицинского мошенничества,
- социальной дискредитации,
- незаконной продажи данных страховым или фармкомпаниям.

Утечка показывает, что даже крупные и авторитетные медицинские учреждения остаются уязвимыми к компрометации данных, когда отсутствует надежная система защиты информации пациентов.

Количество инцидентов с использованием легитимных учетных данных неуклонно растет. Компаниям важно не только заботиться о происходящем в их сети, но и отслеживать утечки данных. Платформа BI.ZONE Brand Protection фиксирует утекшие учетные записи и пароли сотрудников, клиентские базы данных, фрагменты исходного кода и утечки другой чувствительной информации.

Прогнозы, связанные с теневыми ресурсами

Мы проанализировали сообщения на различных теневых ресурсах и сформулировали тренды, которые будут характерны для таких площадок в ближайшее время.



1. Несмотря на активные действия правоохранительных органов, злоумышленники продолжат попытки восстановить работоспособность форумов. Тем не менее правоохранители могут сохранить контроль над некоторыми такими ресурсами, чтобы использовать их для поимки злоумышленников.

2. Злоумышленники начнут искать площадки, альтернативные Telegram, чтобы рекламировать сервисы и продукты, а также обмениваться информацией, так как администрация мессенджера все активнее блокирует их каналы и чаты.

3. Границы классов вредоносного программного обеспечения, которое предлагают на теневых ресурсах, продолжат размываться. Злоумышленники будут предоставлять широкий набор функциональных возможностей в своих разработках.

4. Многие организации будут активно внедрять EDR- и XDR-решения. Это поспособствует развитию теневого рынка продуктов, позволяющих их отключать.

5 Появятся ransomware-as-a-service-программы, которые не будут накладывать ограничения на атаки в тех или иных регионах.

6 Стилеры останутся одним из наиболее популярных классов вредоносного программного обеспечения. Следовательно, аутентификационные данные, полученные с их помощью, продолжат активно распространяться.

7 Несмотря на популярность багбаунти-программ, количество продаваемых 0-day-эксплоитов продолжит расти.

8 Широкий круг лиц продолжит получать на теневых ресурсах доступ к персональным и другим конфиденциальным данным благодаря тому, что информация о компрометации различных организаций активно публикуется.

О компании

BI.ZONE — компания по управлению цифровыми рисками, которая помогает организациям безопасно развивать бизнес в киберпространстве. BI.ZONE разрабатывает собственные продукты для обеспечения устойчивости IT-инфраструктур любого размера и оказывает широкий спектр услуг по киберзащите: от расследования инцидентов и мониторинга угроз до создания стратегий по кибербезопасности и комплексного аутсорсинга профильных функций.

Посмотрите полный список решений на нашем сайте.

800+
защищенных клиентов

850+
успешных расследований

1600+
реализованных проектов

1200+
экспертов по кибербезопасности

ул. Ольховская, д. 4, корп. 2
г. Москва, 105066

Напишите нам:
info@bi.zone

Горячая линия:
+7 499 110-25-34