МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ
КРИМИНАЛЬНАЯ МИЛИЦИЯ

УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ УВД БРЕСТСКОГО ОБЛИСПОЛКОМА

УТВЕРЖДАЮ
Первый заместитель начальника
УВД Брестского облисполкома
полковник милиции
Жигалов И.В.
14.10.2024

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
«Киберохота за несовершеннолетними: методы и мотивы злоумышленников, в онлайн-играх».

БРЕСТ 2024

ВВЕДЕНИЕ

В современном цифровом мире онлайн-игры стали неотъемлемой частью жизни миллионов людей, особенно среди молодежи. Они предлагают увлекательный геймплей, возможность общения с друзьями и новые знакомства.

Однако вместе с ростом популярности виртуальных миров возникает и серьезная проблема — киберохота за несовершеннолетними.

Злоумышленники используют разнообразные методы и манипуляции, чтобы нацелиться на уязвимые группы, извлекая выгоду из доверчивости и неопытности молодых игроков.

Мы рассмотрим ключевые мотивы, стоящие за действиями этих преступников, а также проанализируем их стратегии и тактики, применяемые в онлайн-играх. Понимание этих аспектов является важным шагом к повышению безопасности детей и подростков в виртуальном пространстве.

Справочно:

Skin (скин) *- (англ. - «кожа, шкура, оболочка») - внешний вид игрового персонажа (в некоторых играх оружия).*

Donate (донат) *- (англ. - пожертвование) - пожертвование, которое часто используется для развития приложений или игр (в играх денежные средства используются для усиления способностей игрового персонажа).*

Мод (MOD) игры *- изменение, внесенное в видеоигру. Слово мод является сокращением от модификация. Мод может быть изменением любой части игры, включая то, как она звучит, как она воспроизводится, как она выглядит или что-либо еще. Обычно они создаются фанатами игры, а не людьми, которые создали оригинальную игру.*

Чит, читкод (Cheat) *- cheat «мошенничать, обманывать») — использование сторонней аппаратуры, программ и ошибок игры для обеспечения нечестного преимущества в компьютерных играх.*

Trojan (троян) *- вредоносная программное обеспечение (далее - ПО), которая маскируется под легальное ПО. С их помощью злоумышленники пытаются получить доступ к системе пользователя.*

Backdoor (бэкдор) *- вредоносная программа, предназначенная для скрытого удалённого управления злоумышленником пораженным компьютером.*

Minecraft *- (от англ. mine - «шахта; добывать» + craft - «ремесло; создавать») - компьютерная инди-игра в жанре песочницы, созданная шведским программистом Маркусом Перссоном и выпущенная его студией Mojang AB.*

Roblox *- игровая онлайн-платформа и система создания игр, позволяющая любому пользователю создавать свои собственные и играть в созданные другими игры, охватывающие широкий спектр жанров.*

Among Us *- (с англ. - «Среди нас») — многопользовательская компьютерная игра, разработанная американской игровой студией Innersloth.*

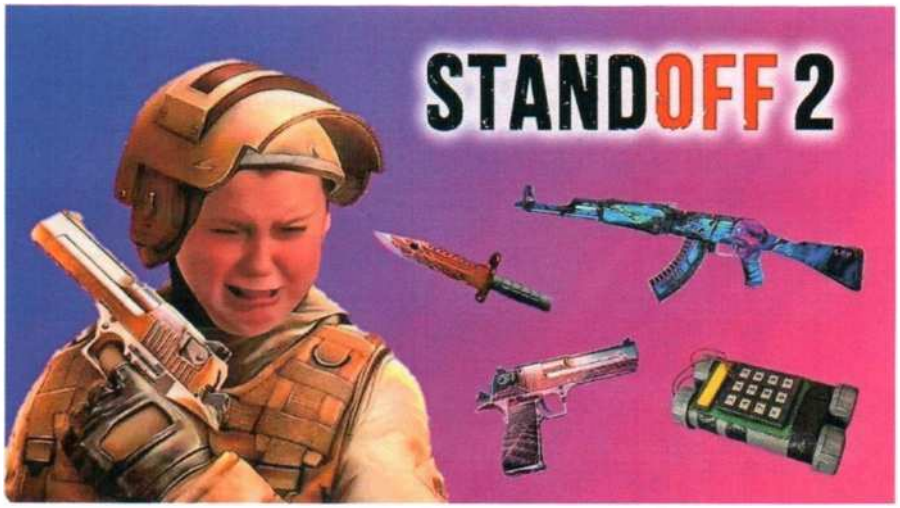
Brawl Stars *- игра для мобильных устройств в жанрах MOBA (многопользовательская онлайн боевая арена) и геройский шутер, разработанная и изданная финской компанией Supercell.*

Five Nights at Freddy's *- (с англ. — «Пять ночей „У Фредди“»), кратко FNaF — франшиза компьютерных игр, созданная разработчиком игр Скоттом Коутоном. Основная серия состоит из компьютерных игр, действие которых происходит в местах, связанных с вымышленной пиццерией «Freddy Fazbear's Pizza», названной так в честь её талисмана — аниматронного медведя Фредди Фазбера.*

Fortnite *- компьютерная онлайн-игра, разработанная американской компанией Epic Games совместно с People Can Fly, предлагает игрокам на выбор три раздельных режима.*

Дети и подростки проводят всё больше времени в киберпространстве, особенно ярко выраженно это в холодную пору года, ведь на улице уже не так просто провести время с друзьями, и многие объединяются в виртуальных мирах за любимыми играми.

Однако мир гейминга далеко не так безобиден, как может показаться на первый взгляд. Игры сами по себе не представляют опасности, но вокруг них часто орудуют мошенники, злоумышленники и киберпреступники.



Исходя из проведенных исследований (последнее из которых проведено экспертами «Лабаратории Касперского») можно определить список наиболее популярных и уязвимых игр, используемых злоумышленниками для своих целей. Ниже предоставлен скриншот, где популярная среди детей и подростков игра «Minecraft» подвергалась кибератакам злоумышленников более 3 миллионов раз.

Название игры	Количество попыток атак
Minecraft	3 094 057
Roblox	1 649 745
Among Us	945 571
Brawl Stars	309 554
Five Nights at Freddy's	219 033
Fortnite	165 859
Angry Birds	66 754

Информация, полученная экспертами «Лабаратории Касперского»

Наиболее распространенными киберугрозами, направленными на несовершеннолетних под видом контента, связанного с видеоиграми, являются загрузчики. Эта тенденция сохраняется на протяжении нескольких лет и затрагивает игры как для детей, так и для взрослых.

Хотя загрузчики сами по себе не являются вредоносными, они часто используются для загрузки других угроз на устройства пользователей. Кроме того, под видом детских игр распространяется рекламное ПО, которое демонстрирует нежелательные или раздражающие всплывающие окна с рекламой на компьютерах и мобильных устройствах.

Киберпреступники также используют различные типы троянских программ, которые маскируются под легальное ПО, чтобы обманом заставить пользователей установить их. После установки такие трояны могут выполнять вредоносные действия без согласия или ведома пользователя. Среди них:

- Trojan-SMS, отправляющий сообщения на платные номера с зараженного мобильного устройства;
- Trojan-Spy, перехватывающий нажатия клавиш, снимки экрана и учетные данные;
- Trojan-PSW, предназначенный для кражи паролей;
-Trojan-Dropper, который устанавливает другие вредоносные программы.

Легкие задания используются как приманка, чтобы заставить детей следовать мошеннической схеме

Чтобы получить желаемый донат (в данном случае игровую валюту) или скин, юным пользователям предлагается ввести логин и пароль от своего игрового аккаунта. Однако вместо получения какого-либо подарка, их игровой аккаунт оказывается украденным мошенниками.

Пользователям предлагается ввести данные своей учетной записи

В игровом мире мошенники используют различные уловки, чтобы обманывать пользователей. Помимо популярных скинов, еще одной распространенной ловушкой является предложение получить игровую валюту.

Один из примеров такого мошенничества обнаружен в игре «Крестный Котец». Пользователям предлагают ввести данные своего игрового аккаунта, а затем пройти опрос, чтобы доказать, что они не являются ботами. После прохождения опроса их перенаправляют на поддельный веб-сайт, который обещает бесплатные призы или раздачи.

Красочный фишинговый сайт посвящен «Крестному Котцу» и ориентирован на детскую аудиторию

Однако на самом деле мошенники не заинтересованы в персональных данных, таких как данные кредитных карт. Они используют видимость игровой активности, чтобы заманить пользователей в другое мошенничество, например, поддельные загрузки, претензии на призы или другие обманные предложения.

Весь процесс представляет собой хитрый способ перенаправить пользователей на другое, более опасное мошенничество под предлогом законного этапа проверки. Таким образом, мошенники пытаются обмануть доверчивых игроков и получить выгоду от их действий.

Фишинговый сайт посвящен игре «ROBLOX» и также ориентирован на детскую аудиторию

Все чаще злоумышленники пытаются обманывать молодую аудиторию, используя различные уловки и ложные обещания. Одним из популярных методов становится предложение получить новый iPhone или даже денежные средства.

Так, на странице одного из telegram сообщества, которая эксплуатировала бренд игры Capybara обнаружена поддельная версия игры, представленная в веб-формате. Пользователям предлагалось зарегистрироваться и сделать депозит, чтобы начать играть и в итоге выиграть IPhone15, или увеличить свою сумму.

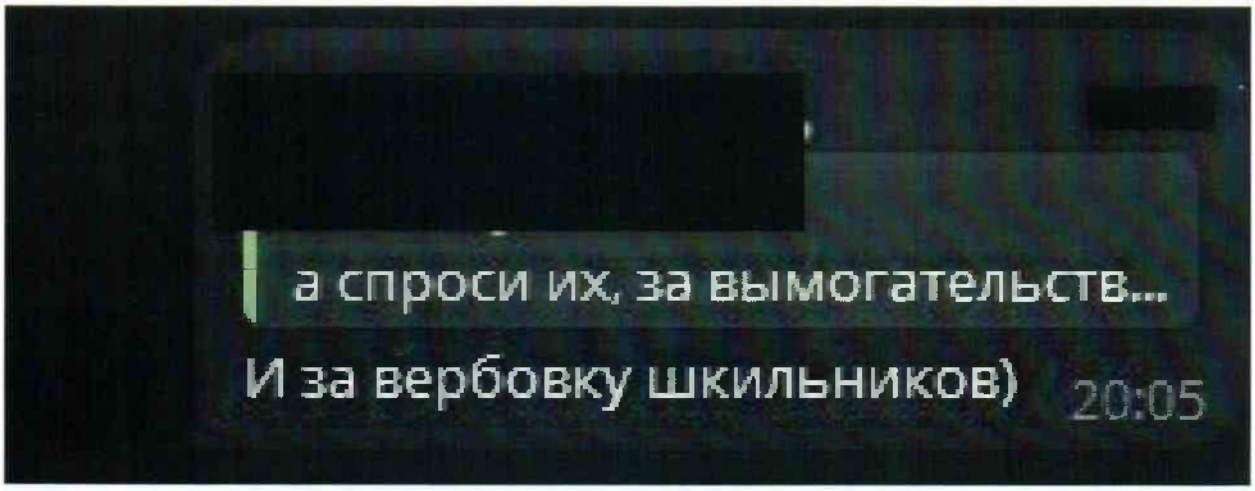
Пользователям предлагают различные поддельные призы под видом одной из игр

Подобные мошеннические схемы становятся все более распространенными, так как злоумышленники пытаются воспользоваться доверчивостью молодых людей и их желанием получить желаемые гаджеты или денежные средства быстрым и легким способом.

Однако на деле за этим стоят лишь обман и хищение личных данных или финансовых средств пользователей.

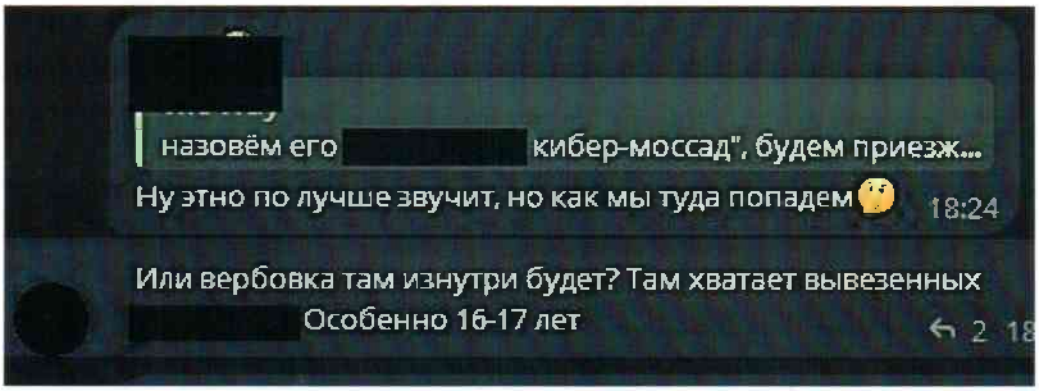
Вербовка детей и подростков в онлайн-играх:

Онлайн-игры, которые так популярны среди детей и подростков, могут быть использованы в качестве площадки для вербовки молодых людей. Злоумышленники применяют различные психологические методы, чтобы завоевать доверие подростков и вовлечь их в противоправную деятельность.



Общение на одном из telegram форумах

Вербовщики могут маскироваться под друзей или наставников, помогая игрокам в игре и постепенно становясь им близкими. Эти отношения могут выглядеть искренними и дружелюбными, что делает их особенно опасными. Подростки могут не подозревать о настоящих намерениях своих "друзей".



Общение на одном из telegram форумах

Злоумышленники также используют игровые элементы, такие как квесты и задания, чтобы замаскировать реальные преступные действия под игровую активность. Молодые люди могут быть втянуты в незаконные действия, не осознавая их истинной природы.

Кроме того, в некоторых играх отдельные игроки или целые сообщества могут оказывать психологическое давление на подростков. Они могут применять методы публичного унижения или отстранения от команды, чтобы вынудить молодых людей совершать определённые действия.

Иностранные вербовщики часто прибегают к финансовым методам воздействия, предлагая реальные деньги или игровую валюту в качестве "подарков" или "заработной платы", чтобы привлечь внимание подростков и вовлечь их в свою деятельность.

Особую опасность представляют вербовщики, которые под предлогом поиска модераторов для игровых сообществ выходят на контакт с подростками.

Они используют методику постепенного вовлечения, начиная с безобидных заданий и постепенно подталкивая молодых людей к совершению все более серьёзных преступлений.

Как юным геймерам оставаться в безопасности:

1. Помогите ребенку создать уникальный, сложный пароль и приучайте его пользоваться надежным менеджером паролей с раннего возраста. Это поможет защитить его аккаунты от взлома.

2. Регулярно обсуждайте с ребенком потенциальные онлайн-угрозы, с которыми он может столкнуться. Объясняйте, как распознавать фишинговые ссылки, вредоносные файлы и другие уловки злоумышленников.

3. Установите на все устройства ребенка надежное программное обеспечение для защиты от киберугроз, особенно если он активный геймер.

4. Будьте в курсе новых мошеннических схем в игровой индустрии и регулярно информируйте об этом ребенка, чтобы он мог распознавать и избегать таких ловушек.

Ключевой момент - вовлекать ребенка в процесс обучения кибербезопасности, а не просто навязывать ему правила. Совместное изучение и обсуждение поможет ему лучше усвоить и применять необходимые знания.

Старший оперуполномоченный по ОВД
УПК КМ УВД Брестского облисполкома
майор милиции А.А.Гулюк
14.10.2024

Начальник УПК КМ
УВД Брестского облисполкома
полковник милиции В.В.Годлевский
14.10.2024

Киберохота за несовершеннолетними: методы и мотивы злоумышленников в онлайн-играх

Слайд 1

Введение

В современном цифровом мире онлайн-игры стали неотъемлемой частью жизни миллионов людей, особенно среди молодежи. Они предлагают увлекательный геймплей, возможность общения с друзьями и новые знакомства. Однако вместе с ростом популярности виртуальных миров возникает и серьезная проблема — киберохота за несовершеннолетними.

Злоумышленники используют разнообразные методы и манипуляции, чтобы нацелиться на уязвимые группы, извлекая выгоду из доверчивости и неопытности молодых игроков. Мы рассмотрим ключевые мотивы, стоящие за действиями этих преступников, а также проанализируем их стратегии и тактики, применяемые в онлайн-играх. Понимание этих аспектов является важным шагом к повышению безопасности детей и подростков в виртуальном пространстве.

Слайд 2

Дети и подростки проводят всё больше времени в киберпространстве, особенно ярко выраженно это в холодную пору года, ведь на улице уже не так просто провести время с друзьями, и многие объединяются в виртуальных мирах за любимыми играми. Однако мир гейминга далеко не так безобиден, как может показаться на первый взгляд. Игры сами по себе не представляют опасности, но вокруг них часто орудуют мошенники, злоумышленники и киберпреступники.

Исходя из проведенных исследований, можно определить список наиболее популярных и уязвимых игр, используемых злоумышленниками для своих целей. Например, популярная среди детей и подростков игра «Minecraft» подвергалась кибератакам злоумышленников более 3 миллионов раз. Наиболее распространенными киберугрозами, направленными на несовершеннолетних под видом контента, связанного с видеоиграми, являются загрузчики. Эта тенденция сохраняется на протяжении нескольких лет и затрагивает игры как для детей, так и для взрослых.

Хотя загрузчики сами по себе не являются вредоносными, они часто используются для загрузки других угроз на устройства пользователей.

Кроме того, под видом детских игр распространяется рекламное ПО, которое демонстрирует нежелательные или раздражающие всплывающие окна с рекламой на компьютерах и мобильных устройствах.

Методы злоумышленников

Слайд 3

Киберпреступники используют различные типы троянских программ, которые маскируются под легальное ПО, чтобы обманом заставить пользователей установить их. После установки такие трояны могут выполнять вредоносные действия без согласия или ведома пользователя. Среди них:

- **Trojan-SMS**: отправляет сообщения на платные номера с зараженного мобильного устройства.
- **Trojan-Spy**: перехватывает нажатия клавиш, делает снимки экрана и собирает учетные данные.
- **Trojan-PSW**: предназначен для кражи паролей.
- **Trojan-Dropper**: устанавливает другие вредоносные программы.

Чтобы получить желаемый донат (в данном случае игровую валюту) или скин, юным пользователям предлагается ввести логин и пароль от своего игрового аккаунта. Однако вместо получения какого-либо подарка, их аккаунт оказывается украденным мошенниками.

Слайд 4

В игровом мире мошенники используют различные уловки, чтобы обманывать пользователей. Например, в игре «Крестный Котец» пользователям предлагают ввести данные своего игрового аккаунта, а затем пройти опрос, чтобы доказать, что они не являются ботами. После прохождения опроса их перенаправляют на поддельный веб-сайт, который обещает бесплатные призы или раздачи. На самом деле мошенники не заинтересованы в персональных данных, таких как данные кредитных карт, а используют видимость игровой активности, чтобы заманить пользователей в другое мошенничество.

Слайд 5

Все чаще злоумышленники пытаются обманывать молодую аудиторию, используя различные уловки и ложные обещания. Одним из популярных методов становится предложение получить новый iPhone или денежные

средства. Например, на странице одного из Telegram-сообществ, эксплуатировавшего бренд игры Capybara, была обнаружена поддельная версия игры, представленная в веб-формате. Пользователям предлагалось зарегистрироваться и сделать депозит, чтобы начать играть и в итоге выиграть iPhone 15 или увеличить свою сумму.

Подобные мошеннические схемы становятся все более распространенными, так как злоумышленники пытаются воспользоваться доверчивостью молодых людей и их желанием получить желаемые гаджеты или денежные средства быстрым и легким способом. Однако на деле за этим стоят лишь обман и хищение личных данных или финансовых средств пользователей.

Вербовка детей и подростков в онлайн-играх

Слайд 6

Онлайн-игры, которые так популярны среди детей и подростков, могут быть использованы в качестве площадки для вербовки молодых людей. Злоумышленники применяют различные психологические методы, чтобы завоевать доверие подростков и вовлечь их в противоправную деятельность. Вербовщики могут маскироваться под друзей или наставников, помогая игрокам в игре и постепенно становясь им близкими. Эти отношения могут выглядеть искренними и дружелюбными, что делает их особенно опасными. Подростки могут не подозревать о настоящих намерениях своих "друзей".

Злоумышленники также используют игровые элементы, такие как квесты и задания, чтобы замаскировать реальные преступные действия под игровую активность. Молодые люди могут быть втянуты в незаконные действия, не осознавая их истинной природы. В некоторых играх отдельные игроки или целые сообщества могут оказывать психологическое давление на подростков, применяя методы публичного унижения или отстранения от команды, чтобы вынудить молодых людей совершать определённые действия.

Иностранные вербовщики часто прибегают к финансовым методам воздействия, предлагая реальные деньги или игровую валюту в качестве "подарков" или "заработной платы", чтобы привлечь внимание подростков. Особую опасность представляют вербовщики, которые под предлогом поиска модераторов для игровых сообществ выходят на контакт с подростками. Они используют методику постепенного вовлечения, начиная

с безобидных заданий и постепенно подталкивая молодых людей к совершению всё более серьёзных преступлений.

Как юным геймерам оставаться в безопасности

Слайд 7

Чтобы защитить детей от киберугроз, родители и опекуны должны принимать активные меры. Вот несколько рекомендаций:

1. **Создание надежных паролей**: Помогите ребенку создать уникальный и сложный пароль, приучая его пользоваться надежным менеджером паролей с раннего возраста. Это поможет защитить его аккаунты от взлома.
2. **Обсуждение онлайн-угроз**: Регулярно обсуждайте с ребенком потенциальные онлайн-угрозы, с которыми он может столкнуться. Объясняйте, как распознавать фишинговые ссылки, вредоносные файлы и другие уловки злоумышленников.
3. **Установите защитное ПО**: Установите на все устройства ребенка надежное программное обеспечение для защиты от киберугроз, особенно если он активный геймер.
4. **Будьте в курсе мошеннических схем**: Регулярно информируйте ребенка о новых мошеннических схемах в игровой индустрии, чтобы он мог распознавать и избегать таких ловушек.

Ключевой момент — вовлекать ребенка в процесс обучения кибербезопасности, а не просто навязывать ему правила. Совместное изучение и обсуждение поможет ему лучше усвоить и применять необходимые знания.

Заключение

Киберохота за несовершеннолетними в онлайн-играх представляет собой серьезную угрозу для безопасности детей и подростков. Злоумышленники используют разнообразные методы и уловки, чтобы манипулировать доверчивыми молодыми игроками, извлекая выгоду из их неопытности. Понимание мотивов и стратегий этих преступников, а также активное участие родителей в обучении детей кибербезопасности — ключевые шаги к созданию более безопасного виртуального пространства для молодежи.

Киберохота за несовершеннолетними в онлайн-играх

В современном цифровом мире онлайн-игры стали неотъемлемой частью жизни миллионов людей, особенно среди молодежи. Они предлагают увлекательный геймплей, возможность общения с друзьями и новые знакомства. Однако, с ростом популярности виртуальных миров, возникает и серьезная проблема — киберохота за несовершеннолетними.

Играй безопасно: угрозы киберпространства в мире онлайн-игр

Дети и подростки проводят всё больше времени в киберпространстве, особенно заметно это в холодное время года.

Мир гейминга очень увлекателен, однако не всегда бывает безопасным. Злоумышленники используют игры для мошенничества, распространения вредоносного ПО и рекламных программ.

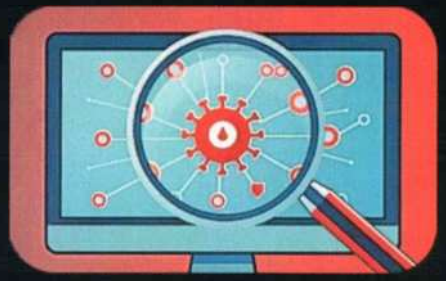
Исследования показывают, что такие популярные игры, как «Minecraft», "Rolox", "Among US"становятся мишенями кибератак, например игра «Minecraft» подвергалась атакам более 3 миллионов раз.

Загрузчики, часто используемые для распространения вредоносного ПО, являются одной из самых распространенных угроз в онлайн-играх.

Темные стороны онлайн-развлечений: типы киберугроз в играх

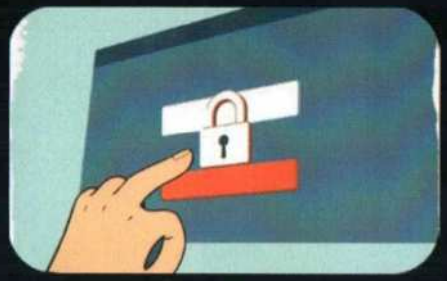
Trojan-SMS

отправляет сообщения на платные номера с зараженного устройства



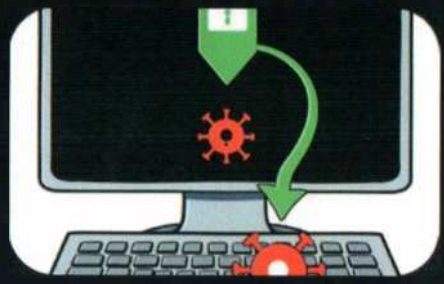
Trojan-Spy

перехватывает нажатия клавиш, снимки экрана и учетные данные



Trojan-PSW

предназначен для кражи паролей



Trojan-Dropper

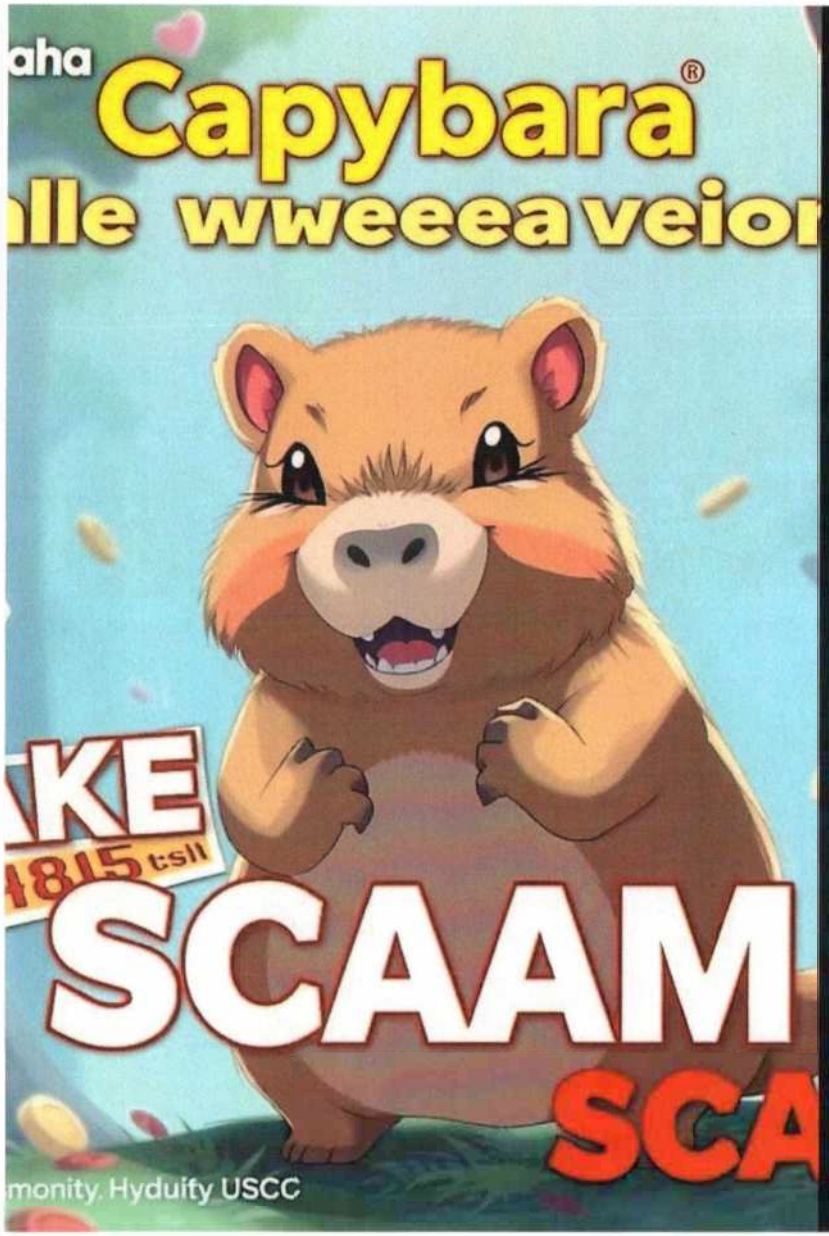
устанавливает другие вредоносные программы

Приманка для доверчивых игроков: мошеннические схемы в играх

Одна из известных схем мошенников - предложение пройти опрос, чтобы доказать, что ты не бот. После этого игроков перенаправляют на поддельный сайт с обещаниями бесплатных призов.

Но на самом деле мошенники лишь пытаются заманить доверчивых пользователей в другие опасные ловушки, например, загрузку вредоносного ПО или участие в фишинговых кампаниях. Хитрые уловки преступников маскируются под легитимные игровые активности.

Будьте бдительны - мошенники готовы на всё, чтобы поживиться за ваш счёт! Всегда проверяйте источники и не доверяйте подозрительным предложениям в играх.



Охотники на доверчивых геймеров

Злоумышленники всё чаще используют онлайн-игры, чтобы выманивать личные данные и деньги у молодой аудитории. Они маскируют свои мошеннические схемы под заманчивые предложения - выиграть новый iPhone или даже наличные.

Так, на странице одного Telegram-сообщества, которая эксплуатировала бренд игры Capybara, была обнаружена поддельная версия игры в веб-формате. Пользователям предлагалось зарегистрироваться и сделать депозит, чтобы начать играть и получить желанный приз.

Но на самом деле за этим стоят лишь обман и кража личных данных или финансовых средств. Будьте бдительны - мошенники готовы на всё, лишь бы поживиться за ваш счёт!

Вербовка детей и подростков в онлайн-играх

Друзья-вербовщики

Вербовщики могут маскироваться под друзей или наставников, помогая игрокам в игре и постепенно становясь им близкими. Эти отношения могут выглядеть искренними и дружелюбными, что делает их особенно опасными. Подростки могут не подозревать о настоящих намерениях своих "друзей".

Игровые ловушки

Злоумышленники также используют игровые элементы, такие как квесты и задания, чтобы замаскировать реальные преступные действия под игровую активность. Молодые люди могут быть втянуты в незаконные действия, не осознавая их истинной природы.

Психологическое давление

В некоторых играх отдельные игроки или целые сообщества могут оказывать психологическое давление на подростков. Они могут применять методы публичного унижения или отстранения от команды, чтобы вынудить молодых людей совершать определённые действия.

Будьте бдительны - мошенники готовы на всё, лишь бы поживиться за ваш счёт! Всегда проверяйте источники и не доверяйте подозрительным предложениям в играх.

Как защитить юных геймеров

Совместная работа

Обсуждайте онлайн-угрозы с ребенком, помогайте ему создавать сложные пароли.

Фишинговые ссылки

Учите ребенка распознавать фишинговые ссылки и вредоносные файлы.

Защита от киберугроз

Устанавливайте на устройства ребенка надежное программное обеспечение для защиты от киберугроз.

Благодарю за внимание!
Помните, никто не останется незамеченным.

TELEGRAM BOT с
профилактическими материалами

HTTPS://T.ME/UPK_BREST_BOT
@UPK_BREST_BOT

SCAN ME