DOI 10.37882/2223-2966.2025.02.16

ОБЗОР ТЕХНИЧЕСКИХ МЕРОПРИЯТИЙ, ПРОВОДИМЫХ ИНТЕРНЕТ-АГРЕССОРОМ ДЛЯ УСПЕШНОГО АКТА КИБЕРБУЛЛИНГА И КОМПЬЮТЕРНЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ

OVERVIEW OF TECHNICAL MEASURES TAKEN BY AN INTERNET AGGRESSOR FOR A SUCCESSFUL ACT OF CYBERBULLYING AND COMPUTER COUNTERMEASURES

I. Krepak

Summary. Scientific article's purpose is to determine current tools and methods for carrying out acts of Internet aggression for a detailed study of manipulations and formation of measures to counteract cyberbullying. Internet bullying incidents from information security point of view occur with various sets of hardware and software, differ depending on intruder's motives, his information security tools knowledge, legitimate and malicious software. Cyber aggressor's separate criterion is the time restrictions, it is due to the hardware resources consumption of devices in operation. Detailed analysis of malware and information systems used was defined as a methodology. Since most acts of Internet bullying in the network space of the CIS countries occur in social networks, there are leaks of personal data and their improper use. To understand effectiveness of pinpoint qualification of information security incidents, the background state of Internet bullying in the school community was analyzed. Correlating current trends with a possible background situation contributes to the correct qualification of events and the selection of corrective technical countermeasures. Modern high school students, despite the high level of background cybercrime and the entertaining nature of such acts, are ready to positively cooperate with educational institutions' administration for passive counteraction. Even though IT development computer attacks' vector expansion, there is a positive trend in the intention to counteract.

Keywords: information security incident, virtual aggression, cyberbullying, OSINT, ISP, indicator of compromise, personal data leak, IS event filters, computer warfare.

Крепак Иван
аспирант, Финансовый университет при Правительстве РФ
krepak.2311@yandex.ru

Аннотация. Целью данной научной статьи стало определение текущего инструментария и методик проведения актов Интернет-агрессии для детального изучения манипуляций и формирования мер по противодействию актам кибербуллинга. Инциденты Интернет-травли с точки зрения информационной безопасности происходят с разнообразными наборами технического обеспечения и программных средств, отличаются в зависимости от мотивов злоумышленника, его знаний средств защиты информации, легитимного и вредоносного программного обеспечения. Отдельный критерий — временные ограничения киберагрессора, он обусловлен потреблением аппаратных ресурсов эксплуатируемых устройств. В качестве методологии был определён детальный анализ применяемого ВПО и информационных систем. Так как большинство актов Интернет-травли на сетевом пространстве стран СНГ происходит в социальных сетях, имеют место быть утечки персональных данных и их нецелевое использование. Чтобы понять эффективность точечной квалификации инцидентов ИБ было проанализировано фоновое состояние Интернет-травли в школьном сообществе. Соотнесение текущих тенденций с возможной фоновой ситуацией способствует корректной квалификации событий и подбора корректирующих технических мер противодействия. Современные старшеклассники, несмотря на высокий уровень фоновой киберпреступности и развлекательный характер подобных актов, готовы позитивно сотрудничать с администрацией учебного заведения для пассивного противодействия. Несмотря на то, что развитие ИТ провоцирует расширение вектора компьютерных атак, наблюдается положительная динамика в намерения по противодействию.

Ключевые слова: инцидент информационной безопасности, виртуальная агрессия, кибербуллинг, OSINT, ISP, индикатор компрометации, утечка персональных данных, фильтры событий ИБ, компьютерное противоборство.

Акт Интернет-агрессии, это противоправное ИТ действие, направленное на кражу личной информации, вывода из строя вычислительного устройства подростка, публикацию личных файлов в общедоступном сетевом пространстве без возможности удаления или сокрытия или побочное мероприятие, где основной жертвой является совершенно другой человек [7, с. 163]. У каждой школы и высшего учебного заведения есть устав, где в большинстве случаев упоминается недопустимость терпимости к актам физической и виртуальной агрессии. К сожалению, у большинства учебных заведений нет кадровых и финансовых возможностей полноценно бороться с Интернет-травлей. Главной самой применяемой мерой на данный момент является пассивное противодействие после того, как акт компьютерной агрессии уже произошёл, но не до [1, с. 70]. Чтобы понимать, как бороться с событиями Интернет-агрессии, необходимо понять, какие техниче-

ские средства применяет хакер и какой стратегии он придерживается.

В данном исследовании Интернет-агрессия в школьной среде изучается с перспективы программных и аппаратных средств, используемых для комплексного акта кибербуллинга. Такой подход позволяет применять предупредительные действия компьютерного противодействия, что окажет позитивное влияние, сократит частоты актов Интернет запугивания и сформирует детальное представление о возможностях реагирования на данные инциденты информационной безопасности.

В рамках этой научной статьи уделяется внимание типовым атакам, направленных на успешную утечку персональных данных и их дальнейшую эксплуатацию. Рассматриваются основные технические мероприятия по борьбе с компьютерной агрессией: опыт российских инженеров информационной безопасности, их иностранных коллег и последствия успешных актов Интернет-травли.

В исследовании приняли участие 197 учащихся обоих полов возрастом от 11 до 14 лет. Несмотря на то, что информация о руководящих принципах и технических методиках проведения актов компьютерных правонарушений, которые сейчас опубликованы на анонимных и теневых форумах, на которые обычному Интернет-пользователю сложно попасть, данные инструкции распространяются очень быстро, видоизменяются и становятся очень успешными в применении.

Существует значительный разрыв между тем, что учащиеся должны знать и текущим масштабом осведомлённости [2, с. 19]. Чтобы решить проблемы, связанные с тем, чтобы идти в ногу с темпами изменений в способах проведения Интернет-агрессорами актов компьютерной травли, необходимо найти подход, опираясь на который, будут налажены типовые и автоматические технические мероприятия и алгоритмы, которые на уровне учётной записей обезвредят подростка от основных киберугроз.

Интерактивные технологии предоставляют подросткам неограниченные возможности для входа в виртуальные сети, социального взаимодействия и исследования новых учебных сред [3, с. 67]. Обычно молодые люди воспринимают веб-активность как чрезмерную свободу. Из-за того, что взрослые, в своём большинстве не обладают ИТ компетенциями, подростки считают их малограмотными. Если рассматривать виртуальную среду с точки зрения взрослого, то Интернет для них, это изолированное место, где дети подвергаются большому количеству различных рисков и им может быть причинён вред [4, с. 16]. Взрослые, в это же время воспринимают виртуальный мир как явление изолирующее и опасное, считая молодых людей подверженными большому риску причинения вреда. Молодые люди стремятся защищать своё сетевое пространство от лишнего внимания старшего поколения [5, с. 205]. Из-за относительно высокого уровня анонимности у злоумышленника есть возможность злоупотреблять возможностями безопасности социальной сети — производить акты Интернет-травли, что не может не беспокоить школьное сообщество.

Интернет-травля это не только пример правонарушения, проводимого с использованием информационных технологий, но и высокотехнологическое действие, направленное на заражение устройств вредоносным ПО, скачивания и модификации персональных файлов [8, с. 44], то есть, полноценная APT-атака направленная на учётную запись подростка или их совокупность (УЗ школьника и его близких друзей). Если обратить внимание на первоначальные шаги, то здесь чаще всего отсутствует этап разведки, так как против известных онлайн платформ применяются готовые шаблоны действий. Например, высокотехнологический фишинг чтобы получить доступ к учётной записи без второго фактора аутентификации.

Технические методы реализации, участники и поверхность кибератаки

Главным рассматриваемым методом стал целевой фишинг с дальнейшим применением анонимайзера. В рамках более масштабного исследования, посвященного изучению особенностей текущих актов Интернет-агрессии, группы преподавателей участвовали в тематических сессиях по темам, изложенным в этом исследовании. Учащиеся занимались совместным обучением во время сессий по сбору данных, рабочие заметки предоставлялись в качестве дополнительных учебных материалов на каждом уроке. Кроме этого, сравнивались точки зрения учащихся с глобальным восприятием проблемы.

В исследовании приняли участие 197 из 456 учеников с седьмого по десятый классы, где 78 из них учатся в седьмом классе, 61 в восьмом, 24 в девятом и 34 в десятом. Они учатся в одной и той же школе. Помимо учеников, в исследовании приняло участие 13 учителей, где 4 преподают 7 классу, трое — восьмому, ещё трое — девятому и так же трое — десятому. Исследование проводилось в 2023 году в одной из столичных школ, где обучается около 1 000 учеников возрастом от 6 до 18 лет. 44 % — дети коренных москвичей, 36 % — из Московской области, а оставшиеся 20 % — дети, чьи родители переехали в Москву из стран ближнего зарубежья. Эти показатели являются важными для школьного населения, охваченного исследованием, в 2009 году.

Технические возможности школы для реагирования на инцидент ИБ, направленные на мониторинг учётной записи ребёнка

Травля определяется как «намеренно оскорбительное поведение, поддерживаемое в течение определен-

ного периода времени отдельным лицом или группой, которое заставляет другого человека чувствовать себя некомфортно или имеет конечную цель — вывести из состояния эмоционального равновесия. Обычно, у школы нет собственного домена, Active Directory и LDAP для AAA. Поэтому, сложно контролировать то, как подростки ведут себя в Интернет-пространстве. Доменная компьютерная инфраструктура позволила бы обеспечить централизированное управление всех технопарком, в течение нескольких минут разворачивать комплексные бинарные пакеты и в режиме реального времени администрировать локальные сервисы.

Так же, в школах, обычно нет DLP и SIEM систем. DLP система позволила бы точечно и быстро определять агрессора и его жертв, перехватывая нажатия клавиш и посещение онлайн сервисов, а SIEM собирал бы детальные логи перемещений вредоносного программного обеспечения по локальной сети. Считается, что ученик играет центральную роль в формировании набора информации, которую он хранит и обрабатывает в сетевом пространстве. Подход школы к борьбе с издевательствами включает в себя ряд стратегий [6, с. 286], в том числе: мониторинговые профилактические, корректирующие (на основании подозрений и логов) и поддерживающие меры (антивирус и другие средства проактивной защиты), а также относительно строгие ограничивающие мероприятия (блокировка доступов и предупреждающие цифровые баннеры).

Рабочие листы были адаптированы из вспомогательных материалов, созданных на основе текущих технических особенностей актов Интернет-агрессии. Случайная выборка была сформирована с помощью учеников классов с разными уровнями ИТ грамотности и различной частотой присутствия в социальных сетях. Темы и краткое содержание раздаточного материала изложены ниже. Школьникам сообщили о существующих программных инструментах, но не говорили, зачем они нужны. Когда подросток не знал ПО, ему предлагалось предположить, к какой профессиональной сфере принадлежит этот инструмент. Это измерялось путем распределения детьми десяти методик использования компьютера и программных продуктов различного характера — как легитимного ПО, так и утилит для сбора эксплоитов (Таблица 1).

Прикладное значение: Ответы относительно десяти технических мер и программных продуктов говорят о том, что, к сожалению, больше половины учеников старших классов правильно определили их принадлежность к инструментарию компьютерного злоумышленника. Следующим этапом стал опрос относительно точечных мероприятий по проведению киберпреступления (Таблица 2), где проверялось, знают ли подростки о мерах и эксплоитах для получения административного управления над хостом жертвы.

Таблица 1.

Технические меры и ПО для проведения актов Интернет-агрессии

Номер	Технические меры и программное обеспечение	Всего, %
1	Использовать не по назначению УЗ компьютера	83
2	Создание сайта, находящегося на анонимном хостинге	75
3	«Яндекс Картинки» с интеллектуальным поиском	66
4	Сервис для приёма СМС на временные номера	65
5	«Proton Mail»	64
6	«Мирай»	63
7	Добавочный код «#31#»	58
8	«Сим-Сими»	53
9	«Metasploit»	49
10	«Зисмо»	45

Таблица 2.

Точечные мероприятия

Номер	Название мероприятия	Всего, %
1	Реверсивный терминал	44
2	«ОСИНТ»	36
3	«Sonarqube»	26
4	Полезная нагрузка	21
5	Радио джаммер	28
6	«nmap»	27
7	«RMS»	22
8	«Radmin»	21
9	«Кейлоггер»	19
10	КИБ	17

Описание результатов: Если в Таблице 1 были обозначены основные меры и программные инструменты для проведения киберпреступлений, которые стали известны из-за массовой культуры, в частности, упоминания в подростковых сериалах про информационные технологии и популярные фильмы про хакеров, то в Таблице 2 приведены более точеные программные решения, о которых подростки могут знать только в двух случаях — интерес к профессии (стремление стать инженером ИБ) или прочитали инструкции по проведению актов компьютерной агрессии. Далее, школьникам был рассказали, что обозначают названия из 2 предыдущих таблиц и обратились с просьбой выбрать меры, которые

позволят обеспечить пассивное противодействие компьютерной угрозе и применить для расследования уже случившегося инцидента информационной безопасности. Были отобраны ученики, которые имеют интерес к информационной безопасности и им заданы вопросы, какие меры следует применять чтобы снизить частоту актов кибербуллинга и предложен список технических мер, которые необходимо выбрать, аргументируя эффективность (Таблица 3).

Таблица 3.

Меры противодействия актам Интернет-травли

Номер	Меры противодействия, выбранные учениками	Всего, %
1	Установка КИБ-систем на всех хостах в школе	35
2	«Suricata» или аналогичное open-source ПО	28
3	Белые и чёрные списки на NGFW	26
4	Теневые УЗ в школьных чатах	13
5	Установка родительского контроля	11
6	Ввод безопасного DNS на уровне сетевого роутеров	21
7	Блокировка ресурсов по доменному имени	31
8	«ОСИНТ» со стороны родителей	28
9	Ограничение Интернет-трафика в мобильном тарифе	17
10	Парсинг целевой УЗ, по ключевым словам,	16
11	Привлечение ИТ поддержки социальных платформ	11

Результаты опроса детей с явным интересом к информационной безопасности в контексте компьютерного противоборства онлайн агрессора и его жертвы говорит о том, что они не имеют активной позиции по этому вопросу, но готовы определять технические средства и мероприятия по пассивному противодействию Интернет-травле. Здесь было сформировано предположение, что данная группа детей, уже определившаяся со своей профессией, имеют высокий толлер к актам компьютерной агрессии.

Далее, после выявления агрессоров Интернет-травли среди первоначальной контрольной группы, им были заданы вопросы относительно предпочтений в технических мерах и ПО для проведения актов кибербуллинга (Таблица 4).

Результаты — У большинства подростков есть осознание того, какими способами и техническими мерами онлайн агрессор осуществляет акты кибербуллинга. Почти половина подростков знают об основных инструментах, которые использует хакер для киберпреступлений и анонимизации своего присутствия. Примерно четверть имеют знания, и, предположительно опыт относительно профессиональных утилит для проведения кибератак. Если считать интерес к специальности «Информационная безопасность» достаточно редким, потому что ею интересуются единицы из тех, кто планирует связать свою жизнь с ИТ профессией, то справедлив вывод о большом количестве скрытых Интернет-агрессорах, имеющих интерес к запланированным актам кибербуллинга и часто читающих тематическую литературу на теневых ресурсах.

Таблица 4.

Точечные мероприятия, инструментарий для актов компьютерной агрессии с точки зрения инициаторов компьютерного правонарушения

Номер	Точечные мероприятия и программное обеспечение	Всего, %
1	Нецелевой фишинг с помощью HTML конструкторов	34
2	Целевой фишинг с загрузкой на собственный FTP-сервер	35
3	Фильтрация сообщений, поиск чувствительных данных	28.5
4	Автоматический парсинг	25
5	Криптосредства для обеспечения анонимности	25.5
6	Ручные ОСИНТ-мероприятия	24
7	Автоматизированный ОСИНТ-парсинг	23
8	Реализация многослойной анонимности	22.5
9	Фишинг многостраничных форм	21
10	Подмена QR-кода для несанкционированной авторизации	17

Киберпреступность

В Таблице 1 представлен перечень точечных мероприятий для осуществления актов Интернет-агрессии с позиции экономии времени и понятного GUI. К сожалению, несмотря на спорную информацию относительно фоновой ИТ грамотности, про которую обычно рассказывают в тематических СМИ, современная молодёжь сильно осведомлена о том, что кибербуллинг это противоправное действие, которое под силу совершить почти любому подростку, имеющему компьютер (или смартфон) и Интернет. Противоположный аргумент, который имеет положительный окрас — продолжительными и запланированными актами кибербуллинга занимается меньшинство. То есть, больше всего мы имеем дело с частными и хаотичными событиями компьютерной агрессии. Если рассматривать борьбу запланированных актов кибертравли менее приоритетной, чем решение проблемы фоновых инцидентов информационной безопасности, то при таком решении, большинство актов Интернет-травли имеют шанс быть относительно рано подавленными.

Средства защиты от точечных мероприятий

В Таблице 2 представлены технические меры и мероприятия, способствующие успешному точечному сбору информации для дальнейшего применения в кибербуллинге. Реверсивный терминал, можно подавить актуальной версией активного антивируса с подпиской. Борьба с «ОСИНТ» мероприятиями почти неэффективна, в качестве профилактики, следует публиковать минимум личной информации в открытом доступе и в групповых переписках. Контрмера против «Sonarqube» и полезной нагрузки — автоматическая проверка загруженных файлов антивирусом. Радио джаммер, к сожалению, подавить почти невозможно. От «nmap» защитит правильно настроенный фаервол. Чтобы понять успешность несанкционированной установки «RMS», «Radmin» или других RAT-приложений следует хотя бы раз в неделю проверять трей и автозагрузку. Кейлоггер можно определить, запустив полное ручное сканирование лицензионным антивирусом. Наличие КИБ определить очень сложно, потому что это легитимное ПО и вендоры стремятся его замаскировать под другое ПО, например — браузер или текстовой редактор.

Обсуждение результатов

В этом исследовании была предпринята попытка определить текущий уровень понимания школьниками проблемы Интернет-травли с точки зрения технического осуществления задачи хакера. К сожалению, результаты, полученные в ходе опроса, схожего с собеседованием в ИТ/ИБ отдел коммерческой организации показало высокую заинтересованность и осведомлённость подростков в средствах и этапах осуществления инцидентов Интернет-агрессии. Другая проблема, которая была определена после анализа результатов анкетирования, это большой разрыв между осведомлённостью в проведении со знаниями по противодействию. То есть, тех, кто знает, как противостоять кибербуллингу техническими мерами почти втрое меньше, чем потенциальных компьютерных злоумышленников.

Заключение

Несмотря на доступность информации о применении вредоносного программного обеспечения и наличие у школьников детальных инструкций по проведению актов Интернет-агрессии проблема может быть частично решена благодаря применению технических контрмер против основных видов компьютерной травли что даст в дальнейшем возможность сфокусироваться на инцидентах информационной безопасности в плоскости социальных сетей, проведение которых больше похоже на заранее запланированную атаку, чем на хаотические попытки получить несанкционированный доступ к файлам, персональным данным и применить в дальнейших мероприятиях злоумышленника. Из-за ограниченности в финансовых ресурсах, наличии кадров и инфраструктурных возможностей, в первую очередь, необходимо обратить внимание на шаблонные атаки.

Современные школьники выросли в цифровую эпоху и воспринимают виртуальный мир совсем не так, как их родители, они обладают бесценными знаниями об использовании и даже злоупотреблении интерактивными технологиями. Аналогично, взрослые имеют доступ к соответствующей информации, но испытывают трудности с ее интерпретацией. Практикующие специалисты пытаются решать возникающие проблемы, консультируясь с подрастающим поколением, поскольку достижения в области технологий открывают новые методы проведения атак Интернет-агрессии, требуется совместный подход, при котором школьники и взрослые активно обмениваются опытом.

ЛИТЕРАТУРА

1. Авдеев А.Ю. Современный подросток в пространстве информационных технологий: психологический аспект. // Вестник Костромского государственного университета. 2012. № 3. С. 67–72.
2. Любов Е.Б. Самоповреждающее поведение подростков: дефиниции, эпидемиология, факторы риска и защитные факторы. // Суицидология. 2019. № 4. С. 16–46.
3. Вараксин А.В. Влияние социальных сетей на формирование ценностных ориентиров современной молодёжи. // Преподаватель XXI века. 2016. № 6. С. 205–212.
4. Бочкарёва Е.В., Стренин Д.А. Правовые аспекты кибербуллинга. // Всероссийский криминологический журнал. 2021. № 1. С. 91–97.
5. Амирова Д.К., Куницына Ю.В. К вопросу об установлении уголовной ответственности за кибербуллинг. // Учёные записки Казанского юридического института МВД России. 2022. № 1. С. 12–16.
6. Серебренникова А.В. Преступления в сфере информационных технологий: кибербуллинг и кибермоббинг. // Проблемы экономики и юридической практики. 2020. № 7. С. 283–287.
7. Чин Ю.А. Уголовно-правовая характеристика кибербуллинга — травли с использованием информационных телекоммуникационных сетей. // ТиПОР. 2023. № 5. С. 160–164.
8. Путинцева А.В. Криминологическая характеристика личности кибербуллера. // Научные исследования. 2020. № 2. С. 42–44.

Журнал «Современная наука: актуальные проблемы теории и практики»