

# Спекуляция пандемией, как преступники используют кризис COVID-19.

Март 2020 г.



## Предисловие

Нынешний кризис является беспрецедентным в истории Европейского Союза (ЕС).

После начала пандемии COVID-19 государства-члены ввели широкие карантинные меры, в том числе ограничения на поездки, ограничения в общественной жизни и закрытие границ.

Однако правоохранительные органы должны выполнять свои обязанности при любых обстоятельствах. Во многих случаях их обязанности даже были расширены для поддержания общественного порядка и безопасности, а также для поддержки органов здравоохранения в их работе. Я хотела бы поблагодарить наших сотрудников здравоохранения, полиции и других ответственных сотрудников за их неустанную и неустанную работу.

Излишне говорить, что эта ситуация также влияет на внутреннюю безопасность ЕС. Преступники быстро воспользовались возможностью использовать кризис, адаптируя свои методы работы или разрабатывая новые виды преступной деятельности. Группы организованной преступности, как известно, являются гибкими и адаптируемыми, и их способность использовать этот кризис означает, что мы должны быть постоянно бдительными и подготовленными.

В настоящее время государства-члены уделяют основное внимание борьбе с кризисом с точки зрения здравоохранения - важно, чтобы мы поддерживали их усилия. Преступность является серьезным подрывным фактором и отвлекает от национальных усилий и усилий ЕС по обеспечению здоровья и безопасности граждан. Вот почему так важно усилить борьбу с преступностью.

Мы в Европоле находимся в постоянном контакте с нашими правоохранительными партнерами по всей территории ЕС и за его пределами. Во время этого кризиса, как никогда ранее, мы должны продолжать оказывать поддержку сотрудникам правоохранительных органов в борьбе с организованной преступностью и терроризмом в целях повышения безопасности граждан Европы.

Опубликованный сегодня отчет содержит обзор того, как преступники адаптируют свои проступки к пандемии COVID-19. Он основан на информации, которую Европол получает от стран-членов ЕС круглосуточно и намерен оказывать поддержку правоохранительным органам государств-членов в их работе.

*КЭТРИН ДЕ БОЛЬ*  
*Исполнительный директор,*  
*Европол*

## Какие факторы влияют на преступления?

Пандемия COVID-19 вынудила национальные правительства и ЕС принять различные меры, чтобы ограничить распространение вспышки, поддержать системы общественного здравоохранения, защитить экономику и обеспечить общественный порядок и безопасность.

Ряд этих мер оказывает существенное влияние на ситуацию с серьезной и организованной преступностью, а также на угрозу со стороны насильственных экстремистов. Чтобы понять влияние пандемии COVID-19 на внутреннюю безопасность ЕС, важно определить факторы, которые вызывают изменения в преступности и терроризме. Эти факторы включают в себя:



# Киберпреступность

## Основные выводы

Глобальная пандемия COVID-19 - это не только серьезная проблема для здоровья, но и риск кибербезопасности. Преступники быстро воспользовались распространением вируса и злоупотребляют спросом людей на информацию и материалы.

Преступники использовали кризис COVID-19 для проведения атак социальной инженерии, а именно фишинга электронной почты посредством спам-ресурсов и более целенаправленных попыток, таких как компрометация деловой электронной почты (BEC).

Существует длинный список кибератак на организации и отдельных лиц, включая фишинговые кампании, которые распространяют вредоносное ПО с помощью вредоносных ссылок и вложений, а также проводят атаки вредоносного ПО и программ-вымогателей, направленные на получение прибыли от глобальной проблемы здравоохранения.

Информация, полученная от партнеров правоохранительных органов, убедительно свидетельствует об увеличении активности в Интернете со стороны тех, кто ищет материалы о насилии над детьми. Это согласуется с публикациями на специализированных форумах и форумах правонарушителей, которые приветствуют возможность взаимодействовать с детьми, которые, как они ожидают, будут более уязвимыми из-за изоляции, меньшего количества надзора и большей активности в Интернете.

Пандемия оказывает влияние на деятельность Darkweb. Некоторые незаконные товары станут дороже, так как исходные материалы станут недоступными. Продавцы на Darkweb предлагают специальные коронные товары (материал для мошенничества) со скидками.

## Перспективы

Количество кибератак значительно, и ожидается их дальнейшее увеличение. Киберпреступники будут продолжать вводить новшества в развертывании различных пакетов вредоносных программ и вымогателей, связанных с пандемией COVID-19. Они могут расширить свою деятельность, включив в нее другие виды онлайн-атак.

Киберпреступники, вероятно, будут стремиться использовать все большее число векторов атак, поскольку все большее число работодателей применяют удаленную работу и разрешают подключения к системам своих организаций.

## **Атака на критически важную инфраструктуру здравоохранения**

Киберпреступники совершили кибератаку на Университетскую клинику Брно в Брно, Чехия, на фоне вспышки COVID-19 в Европе. Поскольку чрезвычайное положение было объявлено в Чехии 12 марта 2020 года, это нападение считалось нападением на критически важную инфраструктуру.

Инцидент побудил больницу отложить срочные операции и перенаправить новых пациентов с острыми заболеваниями в ближайшую альтернативную больницу.

Во время инцидента больница была вынуждена закрыть всю свою ИТ-сеть, а также пострадали два других отделения больницы, Детская больница и Родильный дом.<sup>1</sup>

Эти типы атак во время кризиса в области общественного здравоохранения, такие как пандемия COVID-19, представляют особую угрозу и представляют очень реальный риск для жизни людей.

<sup>1</sup> ZDNet 2020, чешская больница, пострадавшая от кибератаки во время вспышки COVID-19, доступна по адресу <https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/>

## **Мошенничество**

### **Основные выводы**

Мошенники очень быстро адаптировали хорошо известные схемы мошенничества для отдельных граждан, предприятий и общественных организаций.

К ним относятся различные типы адаптированных версий схем телефонного мошенничества, мошенничества с поставками и деактивацией.

Деятельность мошенников будет по-прежнему направлена на увеличение числа жертв по всему ЕС для использования опасений по мере продолжения кризиса.

### **Перспективы**

Мошенничество, связанное с нынешней пандемией, вероятно, очень выгодно для вовлеченных преступников, и они попытаются извлечь выгоду из опасений и страхов жертв в течение всего этого кризисного периода. Можно

ожидать, что в ближайшие недели и месяцы появится большое количество новых или адаптированных схем мошенничества и мошенничества, которые могут нанести существенный финансовый ущерб гражданам, предприятиям и общественным организациям.

Преступники также адаптировали инвестиционные мошенничества для выявления спекулятивных инвестиций в акции, связанные с COVID-19, с обещаниями значительной прибыли.

Можно ожидать появления новых схем мошенничества и дальнейшего увеличения числа жертв. Даже когда нынешний кризис закончится, преступники могут адаптировать схемы мошенничества, чтобы использовать постпандемическую ситуацию.

### **Мошенничество с поставками**

Предприятия, желающие приобрести расходные материалы, такие как защитные маски и другое оборудование, становятся объектом мошенничества.

Расследование одного из государств-членов было направлено на передачу 6,6 млн евро от одной компании к другой в Сингапуре для приобретения спиртосодержащих гелей и масок FFP2 и FFP3. Товар так и не был получен.<sup>1</sup>

В другом случае, о котором сообщило государство-член, компания попыталась приобрести 3,85 миллиона масок и потеряла 300000 евро. Подобные случаи мошенничества с поставками востребованных продуктов были зарегистрированы другими государствами-членами.<sup>2</sup>

<sup>1, 2</sup> Информация Европола.

## **Контрафактные и некачественные товары**

### **Основные выводы**

Распределение контрафактных и / или нестандартных товаров было ключевой областью преступной деятельности в связи с пандемией COVID-19.

Продажа контрафактной медицинской и санитарно-гигиенической продукции, а также средств индивидуальной защиты (СИЗ) и контрафактной фармацевтической продукции увеличилась в разы с начала кризиса. Реклама и



продажа этих товаров осуществляется как в режиме офлайн, так и в автономном режиме.

Некоторые события, такие как распространение поддельных наборов для тестирования на коронавирус, вызывают особую обеспокоенность с точки зрения общественного здравоохранения.

## **Перспективы**

Продажа контрафактных и / или нестандартных товаров в режиме офлайн и в автономном режиме процветает в условиях пандемической экономики. Особенно высок спрос на определенные виды медицинской и гигиенической продукции (маски, перчатки, чистящие средства, фармацевтические продукты), что создало значительный рынок для фальсификаторов продукции, мошенников и спекулянтов.

Количество предложений контрафактных и некачественных товаров будет продолжать расти, особенно в Интернете. Существует риск, что фальсификаторы продукции будут использовать дефицит в поставках некоторых товаров, чтобы все чаще предоставлять контрафактные альтернативы как в автономном режиме, так и в автономном режиме. Это может повлечь за собой некондиционные или контрафактные продукты питания, предметы гигиены и другие товары повседневного спроса.

### **Преступники пользуются высоким спросом на средства гигиены, вызванным вспышкой COVID-19<sup>1</sup>**

Европол поддерживает глобальную операцию с торговлей целевой фальсифицированных лекарственных средств. Операция «Пангея», координируемая Интерполом и охватывающая 90 стран мира, проходила с 3 по 10 марта 2020 года.

Пандемия открыла деловые возможности для наживы преступников. Власти всего мира изъяли почти 34 000 поддельных хирургических масок, наиболее часто продаваемых медицинских изделий в Интернете. Сотрудники правоохранительных органов выявили более 2000 ссылок на продукты, связанные с COVID-19.

Результаты операции свидетельствуют о тревожном росте числа несанкционированных противовирусных препаратов и противомаларийного хлорохина. Витамин С, известный своими иммуностимулирующими свойствами, и другие пищевые добавки были изъяты во всем мире. Обезболивающие и антибиотики также составляли значительную часть конфиската.

### Операция в цифрах

- 121 арест;
- изъято 13 миллионов евро на потенциально опасные лекарственные средства;
- проверено 326 00 упаковок;
- изъято 48 000 упаковок;
- 4,4 миллиона единиц незаконных лекарственных средств, изъятых во всем мире;
- изъято 37 000 несанкционированных и контрафактных медицинских изделий (в основном хирургические маски и наборы для самоконтроля для мониторинга ВИЧ и глюкозы);
- 2 500 удаленных ссылок (веб-сайты, социальные сети, интернет-магазины, реклама);
- было ликвидировано 37 организованных преступных групп.

Европол поддержал эту операцию, содействуя обмену информацией и оказывая аналитическую поддержку.

<sup>1</sup> Европол 2020, Преступники пользуются высоким спросом на гигиенические средства, вызванные вспышкой COVID-19, доступно по адресу <https://www.europol.europa.eu/newsroom/news/rise-of-fake-'corona-cures-revealed-in-global-counterfeit-medicine-operation>

## **Организованная преступность против собственности**

### **Основные выводы**

Различные виды схем, связанных с кражами, совершенными организованной преступностью против собственности, были адаптированы преступниками для использования текущей ситуации. Это включает в себя хорошо известный трюк «племянника» или «внука» и мошенничество с участием представителей государственных органов.

Ожидается, что коммерческие предприятия и медицинские учреждения будут все чаще становиться объектом организованных краж со взломом.

Ожидается, что в период кризиса уровень активности преступников, причастных к организованной преступности против собственности, еще больше возрастет.



## Перспективы

Те же типы краж с использованием обмана, с которыми сталкивались во время кризиса COVID-19, существовали и раньше, но преступники адаптировали свои методы действий к текущей ситуации. Число попыток кражи и мошенничества такого типа, скорее всего, увеличится в ЕС.

Хотя все граждане ЕС подвергаются риску стать жертвами, похоже, что определенные схемы мошенничества особенно направлены на уязвимых членов общества, таких как пожилые люди. Мошенники также обращаются к пострадавшим дома, притворяясь сотрудниками правоохранительных органов или здравоохранения, пользуясь тестированием на COVID-19 и другими предложениями для входа в дома и кражи ценностей.

### Фальсификация и проникновение

Многие государства-члены сообщили о схожем способе совершения кражи. Преступники получают доступ к частным домам, выдавая себя за медицинский персонал, предоставляющий информационные материалы или средства гигиены, или проводя «тест на коронавирус».

Государство-член сообщило о случае, когда преступники позвонили жертве, чтобы сообщить им, что родственник инфицирован и находится в больнице. Они утверждали, что врачи должны будут прийти и немедленно пройти «тест на коронавирус». Эти поддельные врачи пришли к дому жертвы в защитной одежде и масках посреди ночи. Подозреваемые затем взяли очевидный образец мазка изо рта жертвы и вытерли его предплечья очевидными полосками бумаги, чтобы проверить его. Затем ему сказали, что оценка теста займет около пяти часов.

## Иная преступная деятельность

### Основные выводы

Трудно оценить краткосрочное влияние нынешнего пандемического кризиса на рынки наркотиков, но это может изменить динамику спроса и предложения и может нарушить нелегальные каналы поставок. Некоторая отчетность указывает на накопление определенных лекарств потребителями и нехватку снабжения (пре)прекурсорами и основными химическими веществами, используемыми при производстве лекарств в ЕС, что, вероятно, повлияет на выпуск продукции и цены. Эта область требует тщательного контроля,

поскольку нехватка поставок может привести к увеличению числа случаев насилия в связи с наркотиками между конкурирующими поставщиками и дистрибьюторами.

Нелегальная миграция была ключевой проблемой безопасности и гуманитарной помощи для ЕС в течение последних пяти лет и остается таковой во время пандемического кризиса COVID-19. Вероятно, будет повышенный спрос на услуги сетей незаконного ввоза мигрантов для въезда в ЕС или осуществления вторичных перемещений, чтобы обойти усиленные меры пограничного контроля, которые в настоящее время действуют на всей территории ЕС.

Есть некоторые опасения, что закрытие учреждений, предлагающих легальную секс-работу, может увеличить количество случаев сексуальной эксплуатации.

## **Европол оказывает поддержку партнерам по правоохранительной деятельности во время кризиса**

Европол готов поддержать правоохранительные органы государств-членов и других партнеров в течение этого беспрецедентного кризиса.

Европол продолжает оказывать постоянную поддержку в координации расследований между различными государствами-членами и обеспечивает сложную платформу для жизненно важного обмена информацией.

Преступность и терроризм найдут способы продолжать действовать через границы даже во время закрытия границ, и Европол настоятельно призывает наших партнеров обмениваться любыми соответствующими расследованиями и разведанными, чтобы мы могли выявлять трансграничные связи.

Европол продолжает оставаться информационным центром для обмена разведанными между государствами-членами и партнерскими правоохранительными органами. Во времена социального дистанцирования и удаленной работы способность быстро и без усилий обмениваться информацией особенно важна при проведении исследований, основанных на аналитическом результате.

Европол служит платформой для обмена разведанными и предоставляет государствам-членам и другим партнерам такие решения, как Европейская платформа для экспертов (ЕРЕ). Эти решения хорошо совместимы с удаленной работой и являются идеальными инструментами для совместной работы.

## **Стратегическая деятельность**

Предоставление правоохранительным органам государств-членов и нашим партнерам современной ситуационной картины является ключевым приоритетом для Европола во время этого кризиса. Для этого Европол выделяет

ресурсы для постоянного мониторинга ситуации и оказания немедленной поддержки государствам-членам в случае необходимости.

### **Оперативная деятельность**

Протокол экстренного реагирования правоохранительных органов ЕС на крупномасштабные кибератаки.

Возможность крупномасштабной кибератаки с серьезными последствиями в физическом мире и нанесения вреда целому сектору или обществу уже перестала быть немыслима.

Чтобы подготовиться к крупным трансграничным кибератакам, в декабре 2018 года Советом Европейского Союза был принят Протокол о чрезвычайных ситуациях правоохранительных органов Европейского союза (EU LE ERP). Протокол отводит центральную роль Европейскому центру киберпреступности (EC3) Европола и является частью Плана ЕС по скоординированному реагированию на крупномасштабные трансграничные инциденты и кризисы в области кибербезопасности.

EU LE ERP служит инструментом поддержки правоохранительных органов ЕС в обеспечении немедленного реагирования на крупные трансграничные кибератаки посредством быстрой оценки, безопасного и своевременного обмена критически важной информацией и эффективной координации международных аспектов их расследований.

EC3 регулярно проводит координационные совещания по кибернетическому воздействию COVID-19 с агентством ЕС по кибербезопасности ENISA и CERT-EU, группой экспертов по безопасности из институтов ЕС.

### **Профилактические кампании Европола**

Европол продолжает информировать общественность об этих мошенничествах во время пандемии с помощью профилактических кампаний в социальных сетях. Европол предлагает странам работать с нами над формированием и распространением этих сообщений.