КИБЕРПРЕСТУПНОСТЬ И КОРОНАВИРУС COVID19: Риски, Угрозы и Ответные Меры

КЛЮЧЕВЫЕ ПОЛОЖЕНИЯ

- **Пандемия COVID19 способствует росту и распространению киберпреступности.** В то время, как онлайн-мошенничество, вымогательство и сексуальное насилие над детьми в Интернете нацелены на отдельные группы лиц, программы-вымогатели, в первую очередь, подрывают работу организаций, включая больницы. Правительства будут и в дальнейшем становиться мишенью вредоносных программ. Рост распространения ложной, недостоверной информации вводит в заблуждение общественность, а также подрывает эффективность научных мер реагирования.
- **Удаленная работа увеличила число потенциальных жертв киберпреступности. Работая онлайн из дома, люди подвергаются большему риску, тем самым непреднамеренно ставя под угрозу корпоративное программное обеспечение, что делает его более уязвимым для киберпреступников.** Фишинг продолжает предоставлять злоумышленникам, а также другим продвинутым пользователям несанкционированный доступ к системам.
- **В течение большей части 2020 года, количество специалистов по противодействию киберпреступности в правоохранительных органах будет сокращаться. В краткосрочной перспективе количество случаев киберпреступности увеличится, а их жертвы, вероятно, столкнутся с задержками в работе правосудия.** Киберпреступники будут использовать обнаруженные операционные пробелы. Однако, это возможно создаст тактические и стратегические возможности для представителей правоохранительных органов.

Контекст

1. Данный документ представляет краткий обзор рисков и угроз, связанных с киберпреступностью, в контексте пандемии COVID19. Источниками информации для обзора послужили материалы конфиденциальных заседаний правоохранительных органов, УНП ООН, правительств, неправительственных организаций, научных кругов, средств массовой информации; а также материалы из открытых источников и данные партнеров из частного сектора по всему миру, доступные на момент разработки документа (апрель 2020). Рекомендации представлены в конце обзора.

Обзор рисков и угроз: развитие, рост, эксплуатация

2. В настоящее время по всему миру действуют комплексные меры социального дистанцирования. Эти меры привели к значительному увеличению использования средств онлайн-коммуникаций государственными органами, предприятиями и частными лицами. Для многих работа с использованием онлайн-технологий в подобном масштабе непривычна. Данные аудитории представляют собой обширную, привлекательную и уязвимую целевую группу для киберпреступников. В связи с необходимостью удаленной работы и обучения, в Сети все больше пользователей, которые менее осведомлены об угрозах и в большей степени подвергают себя рискам находясь дома, чем на работе или в школе.

3. Киберпреступники усовершенствовали криминальные средства и методы, используя социальные, юридические и психологические нюансы, обусловленные COVID19. Дети школьного возраста, как новые, так и уже активные пользователи Интернета, все чаще становятся мишенью онлайн-преступлений сексуального характера. В частности, преступники проникают в онлайн классы[1] - явление, получившее название „Zoom-бомбинг“ - и используют груминг[2] и сексуальный шантаж[3] в отношении детей.

4. Киберпреступники все чаще используют в своих целях страх людей перед вирусом COVID19: выставляют на продажу в Интернете поддельные лекарственные препараты, несуществующие дезинфицирующие средства, средства индивидуальной защиты (СИЗ), медицинские аппараты и средства гигиены. Другие виды мошенничества включают предложения об инвестиционном консультировании, в том числе по криптовалютам, а также ложные медицинские консультации и диагностику. Один из крупнейших порнографических сайтов предоставил бесплатную подписку пользователям из одной страны, тем самым увеличив риски загрузки вредоносных программ и сексуальных вымогательств.

5. Граждане пожилого возраста, которые зачастую менее осведомлены об опасностях в Интернете, становятся мишенью для киберпреступников, использующих их для загрузки и пересылки вредоносных ссылок через электронные спам сообщения о COVID19, а также в целях распространения ложной информации среди друзей и членов семьи. Киберпреступники продолжают искать новые возможности для вымогательств, утверждая, что они знают и могут раскрыть предполагаемый факт использования жертвой онлайн порнографии.

6. BEC-атаки[4] (атака с использованием компрометации деловой переписки, в которой, как правило, мошенники представляются старшими должностными лицами выбранной в качестве цели организации) продолжают использовать методы социальной инженерии, пользуясь при этом обострившейся ситуацией вокруг пандемии, для перемещения денежных средств на иностранные валютные и криптовалютные счета, а также для получения конфиденциальной информации с целью неправомерного использования, включая шпионаж.

7. На форумах Даркнет продолжают продавать скомпрометированные данные, в том числе высокопоставленных чиновников и знаменитостей. Начинающие киберпреступники ищут совета, как лучше всего использовать пандемию COVID19 для получения прибыли. Известны случаи, когда отдельные киберпреступники пытались отговорить других киберпреступников от DDoS-атак, а также от атак вредоносными программами на больницы и лаборатории по тестированию вакцин. Лица, совершающие сексуальные преступления в отношении детей, продолжают обсуждать какие социальные сети и платформы для обмена фотографиями позволят им получить самый легкий доступ к детям для совершения насилия в их отношении. Преступники также продолжают обмениваться информацией о том, как наилучшим образом определить сотрудников полиции онлайн.

[1] https://techcrunch.com/2020/03/26/norwegian-school-whereby/
[2] https://www.esafety.gov.au/parents/big-issues/unwanted-contact
[3] https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/deal-with-sextortion
[4] https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)

8. Наряду с традиционными видами киберпреступности, передовые целенаправленные угрозы (APT- - Advanced Persistent Threats) продолжают совершенствоваться и использоваться для получения выгоды из ситуации с пандемией COVID19. Основной целью APT атак являются критические объекты инфраструктуры, включая больницы и лаборатории по разработке вакцин. При этом применяются вредоносные программы, программы-вымогатели, а также DDoS-атаки. Мотивом для подобных атак служит не только получение прибыли, но и возможность доступа к персональным данным и другой конфиденциальной информации, представляющей ценность (например, в качестве оперативных/разведывательных данных).

9. Успех большинства киберпреступлений, связанных с COVID19, основан на фишинговых атаках по электронной почте, в качестве первоначального вектора заражения. Как только люди переходят по ссылке или загружают документ, учетная запись становится скомпрометированной. Компрометация учетной записи может быть заметна жертве, но чаще всего она остается скрытой и позволяет установить долгосрочный доступ к учетной записи, организации и связанным с ней программным обеспечением. Помимо сбора конфиденциальной информации, APT атаки могут сорвать работу вебсайтов, вносить изменения в документы, удалять данные, а также распространять ложную информацию.

10. УНП ООН рекомендует правительствам стран и представителям частного сектора активно проводить кампании по повышению уровня информированности населения, с учетом культурной специфики. Горячие линии, позволяющие анонимно сообщать о случаях сексуального насилия над детьми, являются ключевым аспектом ответных мер. Мы также рекомендуем регулярное обновление системы безопасности и резервное копирование данных.

Снижение потенциала правоохранительных органов и социальной устойчивости

11. Во многих странах сотрудники специальных подразделений правоохранительных органов по борьбе с киберпреступностью вынуждены уделять основное внимание не расследованию киберпреступлений, а на поддержку правительственных мер, таких как обеспечение соблюдения карантина во время вспышки коронавируса COVID19. Некоторые специалисты сами стали жертвами болезни. В последующие недели потенциал правоохранительных органов, вероятно, будет продолжать снижаться, негативно сказываясь на способности государств противостоять новым усиливающимся киберугрозам.

12. В некоторых странах нарушено функционирование следственных и судебных процедур из-за необходимости проводить такие мероприятия лично, что не представляется возможным в связи с принятыми местными мерами в области общественного здравоохранения. Другие страны оперативно перешли на судебные процедуры в режиме онлайн.

13. Ложная и недостоверная информация относительно вируса продолжает распространяться, главным образом, через социальные сети, а также через сервисы с зашифрованной передачей сообщений. Социальные сети также столкнулись с проблемой перехода сотрудников на удаленную работу и пытаются справиться с большими объемами дезинформации и фейковых новостей, принимая во внимание внутренние политики компаний и местное законодательство.

14. Дезинформация и кибератаки на важнейшие объекты инфраструктур подрывают общественное доверие и ослабляют эффективность мер для общественной безопасности.

15. УНП ООН рекомендует проведение, по мере возможности, судебных процедур онлайн обеспечивая при этом соблюдение международных стандартов и норм, надлежащих правовых процедур, а также верховенство права.

16. Мы также рекомендуем операторам социальных сетей прилагать больше усилий для борьбы с распространением так называемой «инфодемии» обусловленной COVID19, обеспечивая при этом свободу слова. Наука, основанная на фактах, должна лежать в основе борьбы с COVID19 - мы все играем в этом важную роль.

Анализ

a. Пандемия COVID19 представляет собой беспрецедентный вызов для всего мирового сообщества. Многие перешли от физических операций в режим онлайн, также поступили и преступники. В то время, как масштабы и изощренность киберпреступлений растает, и увеличивается количеств жертв, в некоторых странах представители правоохранительных органов вынуждены исполнять другие обязанности. Усугубляет ситуацию для общественности и правительств экономическое влияние COVID19. Таким образом, складываются идеальные условия для потенциальных киберпреступлений.

b. Угроза киберпреступности, связанная с COVID19, является глобальной проблемой, соответственно ответные меры тоже должны быть глобальными: противодействие киберпреступности в рамках юрисдикции одной страны снижает ее риск во всем мире. Необходимо и впредь проводить обмен информацией о новых угрозах и типах преступлений (Анализ по COVID19 Европол, Оценка киберугроз Интерпол) на международном уровне. Горячие линии, для сообщения о случаях сексуального насилия в отношении детей, являются важным инструментом в борьбе с такими угрозами.

c. Учитывая вероятную нагрузку на упреждающую и оперативную деятельность правоохранительных органов, мы полагаем, что возможность активных расследований случаев киберпреступности в краткосрочной перспективе будет ограничена, в особенности в странах, где такие ресурсы были ограничены еще до начала пандемии. Киберпреступники, в том числе группы APT, будут продолжать использовать ситуацию в своих целях. Публичная отчетность об успешных арестах киберпреступников или предотвращении кибератак, в условиях сегодняшнего кризиса, должна быть усилена, как например недавняя масштабная операция по закрытию/ликвидации 15 серверов для DDoS-атак по найму в Нидерландах[5] в течение одной недели. Это демонстрируют возможности и работу правоохранительных органов, а также напоминает киберпреступникам о том, что операции подобного характера проводятся во всем мире. Активные онлайн-операции под прикрытием против наиболее опасных киберпреступников должны продолжаться. Парадоксально, но киберпреступники могут чаще подвергать себя рискам, полагая, что вероятность их обнаружения снизилась.

[5] https://www.zdnet.com/article/dutch-police-take-down-15-ddos-services-in-a-week/

d. Публичная дипломатия и повышение информированности играют ключевую роль в процессе предотвращения угроз и расширении возможностей, в особенности это относится к уязвимым группам населения - детей и пожилых людей. Меры по борьбе с ложной информацией должны быть транспарентными, предоставляя достоверную и необходимую информацию.

e. Все меры по противодействию с киберпреступностью должны быть пропорциональными, правовыми, подотчетными и обоснованными. Существующие технологии используются многими правительствами для оценки, выявления и отслеживания потенциальных пациентов с COVID19. Эта важная работа должна и впредь проводиться под контролем и четким надзором. Наряду с этим, она должна гарантировать, что меры слежения будут сняты, как только цель борьбы со вспышкой COVID19 будет достигнута. Сейчас настало время для развития доверительных кибер-отношений с общественностью и совместной работы для противодействия насущным угрозам нашего времени, а также укрепления доверия на международном уровне.

f. Сейчас не время для перенаправления обязанностей сотрудников правоохранительных органов по борьбе с киберпреступностью. Способность и потенциал противодействия преступности являются важнейшими компонентами защиты наиболее значимых объектов национальной инфраструктуры, обеспечения безопасности детей в Интернете, расширения возможностей индустрий, обеспечения безопасности больниц и содействия экономическому восстановлению после COVID19.

g. Специалисты УНП ООН по киберпреступности доступны для оказания поддержки и помощи Государствам-членам во всем мире 24 часа в сутки, 7 дней в неделю. Ресурсы УНП ООН по публичной дипломатии доступны по ссылке: https://www.unodc.org/unodc/en/covid-19.html, *включая ссылки на Instagram Live сессии со Специальным Посланником Генерального Секретаря по Делам Молодежи, консультации о мерах киберзащиты для сотрудников ООН UN staff* , а также мероприятия для всех сотрудников Секретариата ООН *iSEEK Live* .

Настоящий документ (UNODC/CMLS/COVID19/Cyber1) может быть распространен без предварительной ссылки на автора.