Научная статья
УДК 343
https://doi.org/10.24412/2073-0454-2023-2-250-252
NIION: 2003-0059-2/23-651
MOSURED: 77/27-003-2023-02-850

Анализ киберпреступности в период пандемии

Наиля Рашидовна Шевко[1], Сергей Яковлевич Казанцев[2], Елена Эдуардовна Турутина[3]
[1,3] Казанский филиал Российского государственного университета правосудия, Казань, Россия
[2] Казанский юридический институт МВД России, Казань, Россия
[1] mos_shev@mail.ru
[2] kaz_s@mail.ru
[3] eturutina@list.ru

Аннотация. Всемирная пандемия COVID-19 наглядно продемонстрировала не только возможности удаленного взаимодействия при помощи современных информационных технологий, но и остро обозначила вопросы обеспечения кибербезопасности — защиты данных, технологий, аппаратных средств от злоумышленников. Пандемийные ограничения способствовали переходу большинства предприятий и организаций на удаленную работу, что повлекло за собой резкий рост киберпреступности. В данной статье анализируются наиболее распространенные в этот период преступные схемы, ущерб от них, а также затраты компаний на обеспечение киберзащиты.

Ключевые слова: киберпространство, пандемия, цифровизация, киберпреступность, кибермошенничество, кибербезопасность, интернет-преступления, киберзащита

Для цитирования: Шевко Н. Р., Казанцев С. Я., Турутина Е. Э. Анализ киберпреступности в период пандемии // Вестник Московского университета МВД России. 2023. № 2. С. 250–252. https://doi.org/10.24412/2073-0454-2023-2-250-252.

Original article

Analyzing cybercrime during a pandemic

Nailya R. Shevko[1], Sergei Ya. Kazantsev[2], Elena E. Turutina[3]
[1,3] Kazan Branch of the Russian State University of Justice, Kazan, Russia
[2] Kazan Law Institute of the Ministry of Internal Affairs of Russia, Kazan, Russia
[1] mos_shev@mail.ru
[2] kaz_s@mail.ru
[3] eturutina@list.ru

Abstract. The global COVID-19 pandemic has clearly demonstrated not only the possibilities of remote interaction using modern information technologies, but also sharply outlined the issues of ensuring cybersecurity — protecting data, technology, and hardware from intruders. Pandemic restrictions have contributed to the transition of most businesses and organizations to work remotely, which has led to a sharp increase in cybercrime. In this article the most common criminal schemes during this period, the damage from them, as well as the costs of companies to ensure cyber defense are being analyzed.

Keywords: cyberspace, pandemic, digitalization, cybercrime, cyberfraud, cybersecurity, internet crime, cyber defense

For citation: Shevko N. R., Kazantsev S. Ya., Turutina E. E. Analyzing cybercrime during a pandemic. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2023;(2):250–252. (In Russ.). https://doi.org/10.24412/2073-0454-2023-2-250-252.

Развитие и внедрение информационных технологий во все процессы жизнедеятельности людей, цифровизация современного общества, к сожалению, не только положительно отразились на жизни человека, но и создали дополнительную угрозу информационной безопасности, стали еще одним действенным ору-

жием в руках злоумышленников. О существовании не только потенциальных, но и реальных угроз кибербезопасности человечество узнало практически одновременно с внедрением компьютерных технологий. Однако пандемия 2020 года усилила это действие. Она показала что, с одной стороны, современные информационные технологии позволили в большинстве случаев не прекращать рабочий цикл предприятия и организации. Объединение (в том числе беспроводное) компьютеров в сети позволило обеспечить дистанционно бесперебойную работу практически всех направлений социально-экономической сферы. С другой стороны, коммуникация посредством киберпространства вносит свои коррективы в обычные, казалось бы, действия. Во главу угла была поставлена кибербезопасность. Киберпреступники воспользовались пандемией COVID-19 и ростом удаленной работы, атакуя как технические, так и социальные уязвимости. Этот исторический рост киберпреступности привел небывалому скачку разнообразия новых преступных схем: от финансового мошенничества с использованием стимулирующих фондов до всплеска фишинговых схем и бот-трафика на фоне растущей волны программ-вымогателей и атак на цепочки поставок программного обеспечения. При этом выросли масштабы и сложность угроз. Причем на международном уровне.

Вопросам исследования кибербезопасности и последствий от этих нарушений сейчас уделяется особое внимание. Так, согласно отчету одной из американских телекоммуникационных компаний [1], крупнейшего поставщика услуг беспроводной связи, компании Verizon, на основе анализа около 30 тыс. инцидентов, зарегистрированных за прошлый год, более 5 тыс. — это подтвержденные утечки данных в 16 различных отраслях четырех регионов мира. Из этих нарушений 86 % были финансово мотивированы. Главным приоритетом в области безопасности является защита конфиденциальных данных.

Согласно отчету ФБР о преступлениях в Интернете Центр жалоб на интернет-преступления (IC3) получил почти на 70 % жалоб больше по сравнению с 2019 годом. Всего было получено около 800 тыс. жалоб, а убытки превысили более $4 млрд. Самыми дорогостоящими атаками являются схемы компрометации деловой электронной почты (BEC): всего было подано порядка 20 тыс. жалоб и убытков порядка $ 2 млрд. К сентябрю 2020 года средний размер выкупа достиг пика почти в $ 200 тыс. долларов, причем подавляющее большинство (86 %) вредоносных программ уникальны для одного ПК, а количество фишинговых атак с января по февраль 2020 года выросло в 5 раз. Фишинг и другие формы социальной инженерии, когда преступники нацелены на людей, а не на технические уязвимости, остаются проверенным методом атаки. По данным IC3 ФБР, по состоянию на 2020 год фишинг является наиболее распространенной атакой киберпреступников. В 2020 году ключевыми факторами фишинга и мошенничества были COVID-19, удаленная работа и технологии. В 2020 году было создано почти 7 млн. новых фишинговых и мошеннических страниц, при этом наибольшее количество новых фишинговых и мошеннических сайтов за один месяц составило более 200 тыс.

В этот период получили широкое распространение такие темы, как ковид, пандемия, подарочные карты, выигрыши, игровые взломщики. В тройку наиболее уязвимых для фишинговых атак отраслей вошли технологии, торговля и финансы. Среди стран, где чаще всего совершались мошенничества, лидируют США, затем Россия и Британские Виргинские острова. Самым популярным почтовым сервисом, используемым для фишинговых наборов, был Gmail.

Неудивительно, что с ростом числа фишинговых атак безопасность электронной почты была признана лучшим проектом в области ИТ-безопасности в 2021 году.

Следующим, получившим наибольшее распространение в сети нарушением можно назвать DDoS-атаки посредством ботнетов. Дело в том, что киберпреступные группы используют ботнеты — автоматизированные наборы скомпрометированных устройств, подключенных к сети, — для нарушения целей с помощью распределенных атак типа «отказ в обслуживании» (DDoS) или повышения эффективности других действий. Это включает в себя рассылку больших объемов спама, масштабную кражу учетных данных или слежку за людьми и организациями.

Ботнеты были проблемой в течение последних нескольких лет, и она становится все хуже. Многие устройства Интернета вещей (IoT) имеют мало или совсем не имеют функций безопасности, и организации часто не следуют рекомендациям по снижению рисков компрометации устройства, тем более, что число сотрудников компаний, работающих удаленно выросло в 3,5 раза — с 20 % до 70 % по всему миру.

Трафик вредоносных ботов составил более 25 % всего трафика веб-сайта в 2020 году, что на 6 % больше, чем в предыдущем году. На долю продвинутых постоянных ботов (APB) в 2020 году приходилось почти 60 % трафика плохих ботов. Это указывает на то, что киберпреступники становятся все более изощренными в использовании ботнетов. Чаще всего трафик вредоносных ботнетов встречается в следующих отраслях:

1) интернет-провайдеры и телекоммуникации (46 %) и информационные технологии (41 %). Как правило, это либо захват аккаунта, либо парсинг, в том числе конкурентных цен;

2) спортивные каналы (34 %). Здесь интересуются коэффициентами ставок и данными о счете;

3) новостные каналы (33 %). Чаще всего встречается мошенничество с рекламой, парсинг пользовательского контента и помещение спама в комментариях;

4) бизнес-услуги (30 %) — сбор данных, захват ак-

каунта, атаки.

В каждом третьем случае боты представлялись мобильными пользовательскими агентами. Рост трафика и, соответственно, объемов передачи данных по телекоммуникационным каналам связи повлек всплеск кибермошенничества. По оценкам экспертов, убытки от киберпреступлений в 2020 году во всем мире составили $1 трлн. При этом атаки со стороны программ-вымогателей участились почти на 40 %, в 6 раз увеличилось число атак вредоносных программ на электронную почту, зафиксирован и рост числа целевых клиентов кибератак (почти на 60 %), удвоился и самый высокий выкуп заложников от программ-вымогателей и достиг $10 млн, что, безусловно, скоординировало затраты компаний на кибербезопасность, защиту данных в сети и предъявило новые требования к обеспечению информационной, экономической и национальной безопасности.

Список источников

1. Verizon Communications [Электронный ресурс] // Официальный сайт Verizon Communications. Режим доступа: https://www.verizon.com/business/?cmp=vcgref (дата обращения: 08.12.2022).

References

1. Verizon Communications [Elektronnyy resurs] // Official website Verizon Communications — Access mode: https://www.verizon.com/business/?cmp=vcgref (Date of reference: 08.12.2022).

Информация об авторах

Н. Р. Шевко — доцент кафедры уголовно-правовых дисциплин Казанского филиала Российского государственного университета правосудия, доцент, кандидат экономических наук;

С. Я. Казанцев — профессор кафедры криминалистики Казанского юридического института МВД России, профессор, доктор педагогических наук;

Е. Э. Турутина — доцент кафедры правовой информатики, информационного права и естественно научных дисциплин Казанского филиала Российского государственного университета правосудия, доцент, кандидат педагогических наук.

Information about the authors

N. R. Shevko — Associate Professor of the Department of Criminal Law Disciplines of the Kazan Branch of the Russian State University of Justice, Associate Professor, Candidate of Economic Sciences;

S. Ya. Kazantsev — Professor of the Department of Criminalistics of the Kazan Law Institute of the Ministry of Internal Affairs of Russia, Professor, Doctor of Pedagogical Sciences;

E. E. Turutina — Associate Professor of the Department of Legal Informatics, Information Law and Natural Science Disciplines of the Kazan Branch of the Russian State University of Justice, Associate Professor, Candidate of Pedagogical Sciences.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

Статья поступила в редакцию 15.12.2022; одобрена после рецензирования 05.02.2023; принята к публикации 10.03.2023.

The article was submitted 15.12.2022; approved after reviewing 05.02.2023; accepted for publication 10.03.2023.