Приложение № 1

Экз. № 1

Выступление заместителя директора НКЦКИ Николая МУРАШОВА на тему: «Защита национального информационного пространства в новых реалиях 2020-2021 гг.»

Слайд № 1 Титульный

В 2020 году наша страна, как и весь мир, столкнулась с новыми вызовами, обусловленными, прежде всего, распространением COVID-19.

Переход на дистанционный режим сказался на обстановке в национальном информационном пространстве и потребовал принятия дополнительных мер по обеспечению его безопасности.

На фоне распространения коронавирусной инфекции и введения ограничительных мер возросло число компьютерных атак. Остановимся на этом подробнее.

Слайд № 2 Пресечение функционирования вредоносных ресурсов

По обращениям НКЦКИ в ушедшем году иностранными партнерами пресечено функционирование более 68 тысяч вредоносных ресурсов. Они располагались в зарубежном адресном пространстве, и с них осуществлялись компьютерные атаки на информационные системы Российской Федерации.

По запросам иностранных партнеров в информационном пространстве Российской Федерации пресечено функционирование более 9 тысяч вредоносных ресурсов.

Наши оценки географического распределения источников компьютерных атак подтверждаются сведениями зарубежных компаний в сфере информационной безопасности. Они приведены в раздаточном материале. Его Вы сможете загрузить на сайте Пресс-центра.

При этом в геополитических интересах одним из основных источников угроз в информационном пространстве безосновательно называют Российскую Федерацию.

Слайд № 3 Взлом ПО компании SolarWinds

В декабре 2020 г. стало известно о взломе программных продуктов компании SolarWinds. Данной теме мы могли бы посвятить отдельную встречу, поэтому сегодня обращу Ваше внимание на наиболее яркие факты, предоставляющие пищу для дальнейших размышлений и исследований.

В частности на особенности развития рынка ИКТ, а также на некоторые из «просчетов» в обеспечении информационной безопасности, которые создали условия для осуществления компьютерной атаки.

Слайд № 4 Монополизация рынка ИКТ

Уязвимость глобального информационного пространства во многом является следствием монополизации рынка IT - технологий. В отличие от европейской или китайской стратегии развития, американские корпорации активно борются с конкурентами, поглощают все перспективные инновационные старт-апы.

Главным «поглотителем» является группа ведущих IT компаний, известная как GAFAM.

Из-за монополизации информационные технологии становятся все более унифицированными, а цифровая среда – типовой. Достаточно просчета или ошибки разработчика, чтобы критическая уязвимость программного обеспечения была растиражирована по всему миру.

Слайд № 5 Проблемы унификации цифровой среды

Риски эксплуатации таких уязвимостей «типовыми эксплойтами» растут экспоненциально, поскольку связанность и взаимозависимость технологий очень высока. Безопасность миллионов пользователей поставлена в зависимость от добросовестности и ответственности компаний-производителей.

Экономическая выгода для бизнеса стоит на первом месте. Пример с компанией SolarWinds это наглядно продемонстрировал.

Необходимо отметить, что атакованное программное обеспечение было развернуто без соблюдения требований безопасности.

Слайд № 6 Расследование инцидента с Solarwinds

Благодаря расследованию инцидента стало известно, что еще в 2017 году сотрудник компании SolarWinds Йен Торнтон-Трамп предупреждал

о существовавших проблемах с обеспечением кибербезопасности, но не был услышан. Уже тогда данные для доступа к программному обеспечению для дистанционного управления SolarWinds были доступны в Darknet.

КЛИК

Другие подробности, говорящие о системном характере проблем с контролем безопасности, сообщило Reuters. Благодаря исследованиям Винота Кумара, стало известно о том, что пароль доступа к серверу обновлений вопреки общеизвестным рекомендациям был примитивным.

Кроме того, странно выглядит и рекомендация SolarWinds отключать антивирусные средства при установке обновлений ее программного обеспечения.

Возвратимся к предпринимаемым НКЦКИ мерам по защите национального информационного пространства.

Слайд № 7 Повышение осведомлённости пользователей об актуальных угрозах

В целях повышения осведомленности российских пользователей об актуальных угрозах и доведения практических рекомендаций по их нейтрализации Центр обеспечивает функционирование портала «Безопасность российских пользователей в сети Интернет» (http://www.safe-surf.ru).

Слайд № 8 Информирование об угрозах безопасности и рекомендациях по их нейтрализации

В начале пандемии COVID-19 Центр провел анализ новых угроз компьютерной безопасности и опубликовал на Портале рекомендации по противодействию им и обеспечению информационной безопасности в условиях дистанционного режима работы.

Слайд № 9 Информирование об актуальных уязвимостях ПО и угрозах безопасности

С 2019 г. Центр проводит большую работу по анализу уязвимостей программного обеспечения и выявлению угроз безопасности информации. Результаты этой работы содержатся в тематических бюллетенях. Их количество в 2020 г. увеличилось практически в три раза по сравнению с предыдущим годом.

Своевременная подготовка и опубликование бюллетеней позволили предотвратить реализацию угроз на объектах информационной инфраструктуры.

В прошедшем году не допущены компьютерные инциденты, затрагивающие систему государственного управления или экономику страны и ближайших союзников.

КЛИК

Бюллетени содержат необходимую информацию об уязвимостях и программных ошибках, а также рекомендации по их устранению.

Сейчас ознакомиться с ними может любой пользователь сети Интернет.

Слайд № 10 Изменение обстановки в информационном пространстве

Далее подробнее остановимся на обстановке в национальном и глобальном информационном пространстве. На ее формирование в этот период времени оказывали влияние два фактора:

– повышенное внимание средств массовой информации к теме пандемии;

– карантинные мероприятия, которые привели к изменению устоявшегося режима функционирования систем в сети Интернет. Это создавало лавинные нагрузки на глобальную сеть связи и могло приводить к кратковременным сбоям.

Слайд № 11 Единичные факты недоступности информационных систем общего пользования

Фактически пандемия сформировала условия для проверки качества функционирования информационной инфраструктуры и сервисов.

В частности, отмечались единичные факты недоступности государственных информационных систем общего пользования таких, как mos.ru, стопкоронавирус.рф, а также периодическое зависание портала школьных домашних заданий – uchi.ru.

Слайд № 12 Объем глобального трафика сети Интернет

Аналогичные перегрузки отмечались не только в нашей стране, но и во всем мире. С начала карантинных мероприятий многие зарубежные провайдеры сообщали о повышении объема трафика на треть, а некоторые даже в два раза.

Подобные проблемы возникали и с сетевыми приложениями. Например, в Китае в феврале 2020 г. использование видеоконференций возросло в 22 раза по сравнению с 2019 г. Весомый вклад внесли и оставленные дома школьники: игровая сеть Steam известила о более чем 20 миллионах «геймеров», вошедших в систему одновременно.

Кроме того, сформировавшаяся в эпоху пандемии обстановка в национальном информационном пространстве характеризовалась ростом количества и сложности компьютерных атак.

Слайд № 13 Основные цели компьютерных атак

Проведенный НКЦКИ анализ данных показал, что если в 2019 году наибольшая доля компьютерных атак была нацелена на кредитно-финансовую сферу – 33 %, то в 2020 году – на информационные ресурсы органов государственной власти и предприятий промышленности.

Так доля атак на информационные ресурсы органов государственной власти возросла с 27% до 58 %, предприятий промышлености – с 18% до 38 %.

Далее подробнее остановимся на основных типах выявленных компьютерных атак.

Слайд № 14 Примеры компьютерных атак методом социальной инженерии

Созданный вокруг COVID-19 информационный фон привел к росту числа компьютерных атак методом социальной инженерии, в которых в качестве «приманки» использовалась тема коронавирусной инфекции. В состоянии стресса люди становились крайне восприимчивыми к мошенническим уловкам хакеров, использовавших в своих интересах сформировавшиеся под воздействием пандемии новые реалии.

За последние две недели марта 2020 г. количество компьютерных атак методом социальной инженерии возросло в 10 раз.

Примеры таких компьютерных атак:

– рассылка писем по электронной почте с вредоносным вложением или ссылкой на вредоносную программу или сайт, как правило, с целью фишинга или

вымогательства. Источники таких писем маскируются под официальные организации, например, Всемирную организацию здравоохранения, страховую или благотворительную некоммерческую компанию и тому подобное. Основными целями таких атак являлось получение доступа к конфиденциальной информации, персональным данным и номерам банковских карт;

КЛИК

– попытки установки вредоносных приложений. Например, через карты распространения коронавируса с указанием вымышленных вирусоносителей;

Слайд № 15 Примеры компьютерных атак методом социальной инженерии

– посещение фейковых веб-порталов, замаскированных под организации здравоохранения, страховые компании и т.д.;

КЛИК

– создание фейковых новостей, ссылающиеся на вредоносные ресурсы. Например, о районе местонахождения, срочных сообщениях органов государственной власти, о генерации карантинного QR-кода и т.д.

Слайд № 16 Нарушение конфиденциальности в системах телемедицины

Относительно новым объектом компьютерных атак методом компрометации персональных данных стали системы телемедицины, популярные при лечении на дому.

Слайд № 17 Компьютерные атаки на информационные ресурсы ФБУН ГНЦ ВБ «Вектор»

Несмотря на насаждаемый в иностранных СМИ тезис о неэффективности российской вакцины от COVID-19, в период ее создания зафиксировано четырехкратное увеличение количества компьютерных атак на информационные ресурсы разработчика.

Все компьютерные атаки на один из крупнейших научных вирусологических и биотехнологических центров России «Вектор» были направлены на организацию несанкционированного доступа, что свидетельствует об устремлениях к получению технологий создания вакцины от COVID-19.

Слайд № 18 2020: увеличение крупномасштабных DDoS-атак на российские информационные ресурсы

В рассматриваемый период, как и прежде, оставалась актуальной проблема атак типа «отказ в обслуживании». При этом их количество значительно возросло.

КЛИК

Существенное увеличение числа вредоносных ресурсов в зарубежном адресном пространстве, функционирование которых было прекращено в 2020 году, связано с проведением крупномасштабных DDoS-атак на российские информационные системы.

Слайд № 19 DDoS-атаки в период проведения несанкционированных акций протеста

DDoS-атаки использовались в том числе и в экстремистских целях.

Так зафиксирован рост количества компьютерных атак такого типа на официальные информационные ресурсы органов государственной власти Российской Федерации в период проведения несанкционированных акций протеста в поддержку Навального.

Атакам подверглись официальные сайты МИД,

КЛИК

Минтруда, Минэкономразвития, Генпрокуратуры и Росгвардии России. Источники вредоносного воздействия располагались, в том числе, в адресном пространстве США.

Заметим, что в разные дни атаки проводились по одному и тому же сценарию.

Слайд № 20 Компьютерная атака на ЦОДД Нижнего Новгорода

Подобные мероприятия сопровождались и другими «аккомпанементами» в информационном пространстве.

В частности, в январе 2020 года был атакован сайт Муниципального казенного учреждения «Центр организации дорожного движения Нижнего Новгорода». После получения несанкционированного доступа на ресурсе были размещены фотография Навального и текстовое сообщение о том, что атака была

проведена в его поддержку. Вредоносное воздействие было осуществлено с ip-адресов Франции и Германии.

Приведенные примеры свидетельствуют о том, что заявляемые координаторами и волонтерами движения и штаба Навального «спонтанность» и «народность» акций протеста в его поддержку не соответствуют действительности.

Слайд № 21 Титульный

Отметим, что своевременно принятые Центром меры позволили не допустить нарушения функционирования официальных ресурсов российских органов государственной власти.

Адаптируясь к реалиям 2020-2021 гг., НКЦКИ продолжает выявлять новые угрозы информационной безопасности и разрабатывать меры по их нейтрализации.

Спасибо за внимание.