Ответы «Ростелеком-Солар» на вопросы, заданные в ходе вебинара

1) Откуда поступает большинство кибератак на российский сектор?

Сложно говорить со 100% уверенностью, поскольку злоумышленники, особенно опытные, атакуют компании не со своего компьютера, а используя промежуточные сервера, которые могут располагаться в любой стране мира. То же самое касается серверов, на которые отправляет информацию вредоносное ПО. Поэтому атрибуция атаки, т.е. отнесение ее к конкретной группировке, всегда производится на основе множества признаков.

По данным центра мониторинга и реагирования на кибератаки Solar JSOC за 2020 год, в 40% случаев целью атак высокопрофессиональных хакерских группировок, в том числе работающих в интересах иностранных государств, является доступ к промышленным сегментам предприятий. Кроме того, мы наблюдаем серьезный рост атак на объекты КИИ. Он не столь значителен, как рост киберугроз в целом по России, но следует помнить, что именно атаки на КИИ, как правило, сложнее всего в выявлении и противодействии.

2) Какие решения по защите АСУТП есть сейчас в портфеле «Ростелекома»? Насколько развито сотрудничество Schneider с «Ростелекомом» в этом направлении?

Лаборатория кибербезопасности АСУ ТП компании «Ростелеком-Солар» и Schneider Electric сотрудничают в части выявления и устранения уязвимостей в элементах создания промышленных сетей — специализированном программном и аппаратном обеспечении. «Ростелеком» не разрабатывает собственные решения по защите АСУ ТП, но реализует комплексные проекты по обеспечению информационной безопасности промышленных сегментов предприятий.

3) Каковы цели и типы кибератак на предприятия МСБ? Какими могут быть потери компаний?

МСБ чаще атакуют киберпреступники невысокого уровня квалификации, так называемые киберхулиганы и кибернаемники, которые могут работать по заказу конкурентов или в расчете на быстрый вывод финансовых средств из слабо защищенной организации.

СТАТИСТИКА КИБЕРАТАК

Статистика кибератак за 2020 год находится в процессе подготовки и будет озвучена в конце марта – начале апреля 2021 года. Предлагаем данные за 2019 год:

Статистика кибератак в Приволжском федеральном округе

За 2019 год центр мониторинга и реагирования на киберугрозы Solar JSOC компании «Ростелеком» выявил и отразил свыше 1,1 млн внешних атак на информационные ресурсы организаций. При этом традиционно наибольшее число инцидентов такого рода – более 430 тысяч – было выявлено в Москве. В Приволжском федеральном округе за год было зафиксировано свыше 77 тысяч атак.

Наибольшее количество атак в регионе (43%) было реализовано с помощью вредоносных программ (вирусов, троянов, шпионского ПО и т.п.), тогда как в среднем по стране этот показатель равен 33%. Как отмечают эксперты Solar JSOC, этим инструментарием хакеры пользуются все активнее – в 2019 году количество киберпреступлений с использованием вредоносов выросло на 11%, причем преступники постоянно их совершенствуют, делая все менее заметными для средств защиты.

Вторым по популярности методами взлома инфраструктуры организаций в регионе стало использование уязвимостей в веб-приложениях (веб-порталах, электронной почте, интернет-банках, личных кабинетах и т.д.). На эти виды атак приходится 29 % всех инцидентов. На третьем месте – подбор и компрометация учетных данных (логинов и

паролей) от интернет-ресурсов организаций (14%).

Среди прочих типов кибератак, осуществлявшихся на компании Приволжского федерального округа, эксперты Solar JSOC выделяют попытки компрометации логинов и паролей системных администраторов, DDoS (атаки, приводящие к недоступности веб-сайтов) и эксплуатацию известных уязвимостей, которые не были своевременно устранены службами информационной безопасности организаций.

«Хотя по объему киберинцидентов Поволжье стоит далеко не на первом месте, здесь также имеется достаточно сильная «уязвимость» — слабая осведомленность населения в вопросах обеспечения информационной безопасности. Этот показатель в Приволжском федеральном округе ниже, чем в целом по стране, что открывает перед хакерами больше возможностей, например, для фишинга – вредоносных рассылок на электронную почту. Как показывает статистика, в среднем каждый пятый пользователь в регионе открывает такие письма или поддается другим способам социальной инженерии, за счет чего преступники могут легко проникнуть в информационную инфраструктуру организации. Лучшая мера профилактики в данном случае – повышение киберграмотности сотрудников», — поделился ***Владимир Дрюков, директор центра мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком».***

Статистика кибератак в Дальневосточном федеральном округе

За 2019 год центр мониторинга и реагирования на киберугрозы Solar JSOC компании «Ростелеком» выявил и отразил свыше 1,1 млн внешних атак на информационные ресурсы организаций. При этом традиционно наибольшее число инцидентов такого рода – более 430 тысяч – было выявлено в Москве. В Дальневосточном федеральном округе за год было зафиксировано свыше 115 тысяч атак.

На Дальнем Востоке самыми распространенными в 2019 году стали атаки на веб-приложения (веб-порталы, электронную почту, интеренет-банки, личные кабинеты и т.д.). С подобными действиями злоумышленников организации сталкивались в 34% случаев. Этот метод атаки показывает рост и в целом по стране. По данным Solar JSOC, количество инцидентов, связанных с веб-приложениями, за 2019 год увеличилось на 13%.

«Такая динамика может быть связана с активным развитием корпоративных интернет-ресурсов, причем не только в традиционных для этого отраслях (банках, ритейле), но и в энергетике или госсекторе. При этом большая часть из них имеет критические уязвимости, позволяющие получить привилегированный доступ к ресурсам организации», – пояснил ***Владимир Дрюков, директор центра мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком».***

Вторым по популярности методом взлома инфраструктуры организаций региона стало распространение вредоносного ПО (вирусы, трояны, шпионское ПО и т. п.) – 32% от общего количества инцидентов. По оценке экспертов Solar JSOC, в большинстве случаев злоумышленники используют фишинг для доставки вредоносного ПО на компьютер жертвы. При этом более трети фишинговых рассылок в регионе в 2019 году содержали в себе вирусы-шифровальщики. Попадая на компьютер жертвы, этот вредонос шифрует ценные данные, чтобы их невозможно было открыть, а за расшифровку злоумышленники, как правило, требуют выкуп.

Среди прочих типов кибератак, осуществлявшихся на компании региона, эксперты Solar JSOC выделяют подбор и компрометацию учетных данных от интернет-ресурсов

организаций, попытки компрометации логинов и паролей системных администраторов, DDoS (атаки, приводящие к недоступности веб-сайтов) и эксплуатацию известных уязвимостей, которые не были своевременно устранены службами информационной безопасности организаций.

Статистика кибератак в Северо-Западном федеральном округе

За 2019 год центр мониторинга и реагирования на киберугрозы Solar JSOC компании «Ростелеком» выявил и отразил свыше 1,1 млн внешних атак на информационные ресурсы организаций. При этом традиционно наибольшее число инцидентов такого рода – более 430 тысяч – было выявлено в Москве. В Северо-Западном федеральном округе за год было зафиксировано свыше 128 тысяч кибератак.

Самым распространенным инструментом злоумышленников в регионе в 2019 году стало использование уязвимостей в веб-приложениях (веб-порталах, электронной почте, интернет-банках, личных кабинетах и т.д.). На этот вид атак приходится 36% всех инцидентов. При этом, как отмечают эксперты Solar JSOC, в Северо-Западном федеральном округе отчетливо прослеживается одна из самых высоких динамик уязвимостей веба: каждое третье приложение в области исследования имеет возможность взлома и получения доступа к серверу организации.

Этот метод атаки показывает рост и в целом по стране. По данным Solar JSOC, количество инцидентов, связанных с веб-приложениями, за 2019 год увеличилось на 13%. «Такая динамика может быть связана с активным развитием корпоративных интернет-ресурсов, причем не только в традиционных для этого отраслях (банках, ритейле), но и в энергетике, ТЭК, госсекторе. При этом большая часть подобных ресурсов имеет критические уязвимости, позволяющие получить привилегированный доступ к ресурсам организации», – пояснил ***Владимир Дрюков, директор центра мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком».***

Также в 28% случаев киберпреступники использовали внедрение вредоносных программ (вирусов, троянов, шпионского ПО и т.п.) в информационную инфраструктуру организаций региона. В целом по стране количество таких атак в 2019 году выросло на 11%. При этом хакеры постоянно совершенствуют свои инструменты, делая зловреды менее заметными для средств защиты.

На третьем месте в арсенале злоумышленников, атаковавших регион, оказался метод подбора и компрометации учетных данных (логинов и паролей) от интернет-ресурсов организаций. Данный инструмент применялся в почти 20% случаев. Среди прочих типов кибератак, осуществлявшихся на компании региона, эксперты Solar JSOC выделяют попытки компрометации логинов и паролей системных администраторов, DDoS (атаки, приводящие к недоступности веб-сайтов) и эксплуатацию известных уязвимостей, которые не были своевременно устранены службами информационной безопасности организаций.

Статистика кибератак в Сибирском федеральном округе

За 2019 год центр мониторинга и реагирования на киберугрозы Solar JSOC компании «Ростелеком» выявил и отразил свыше 1,1 млн внешних атак на информационные ресурсы организаций. При этом традиционно наибольшее число инцидентов такого рода – более 430 тысяч – было выявлено в Москве. В Сибирском федеральном округе за год было зафиксировано свыше 110 тысяч атак.

Наибольшее количество (более 34%) атак на организации региона было реализовано с помощью вредоносных программ (вирусов, троянов, шпионского ПО и т.п.). Как отмечают эксперты Solar JSOC, этим инструментарием хакеры пользуются все активнее – в 2019 году количество инцидентов с применением вредоносов выросло на 11%, причем преступники постоянно их совершенствуют, делая все менее заметными для средств защиты.

Вторым по популярности методом взлома инфраструктуры организаций Сибири стала эксплуатация уязвимостей веб-приложений (веб-порталов, электронной почты, интернет-банков, личных кабинетов и т.д.). Этот вариант злоумышленники использовали в 31% случаев. На третьем месте – подбор и компрометация учетных данных (логинов и паролей) от интернет-ресурсов организаций – их доля составляет 17,5% от общего количества атак.

Среди прочих киберинцидентов в компаниях Сибирского федерального округа эксперты Solar JSOC выделяют попытки компрометации логинов и паролей системных администраторов, DDoS (атаки, приводящие к недоступности веб-сайтов) и эксплуатацию известных уязвимостей, которые не были своевременно устранены службами информационной безопасности организаций.

«Отличительной особенностью региона является то, что более 20% атак на объекты критической информационной инфраструктуры были направлены на проникновение в автоматизированные системы управления промышленными объектами (АСУ ТП). В среднем по стране этот показатель равен 16%. Данная ситуация связана с низким уровнем кибергигиены и отсутствием в инфраструктуре организаций сегментирования сетей на корпоративные и технологические», – отметил ***Владимир Дрюков, директор центра мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком».***

Статистика кибератак в Уральском федеральном округе

За 2019 год центр мониторинга и реагирования на киберугрозы Solar JSOC компании «Ростелеком» выявил и отразил свыше 1,1 млн внешних атак на информационные ресурсы организаций. При этом традиционно наибольшее число инцидентов такого рода – более 430 тысяч – было выявлено в Москве. В Уральском федеральном округе за год было зафиксировано свыше118 тысяч кибератак.

Примерно треть (32%) всех инцидентов на Урале связана с распространением вредоносного ПО (вирусы, трояны, шпионское ПО и т.п.). Как отмечают эксперты Solar JSOC, данным инструментарием хакеры пользуются все активнее – в 2019 году количество инцидентов с применением вредоносов выросло на 11%. Этому способствует развитие почтового фишинга как основного способа доставки зараженного ПО.

«Особенностью региона является то, что в большинстве случаев преступники использовали фишинг для доставки майнингового ПО на компьютер жертвы. По нашим оценкам, более чем в 70% случаев компании не в курсе, что их вычислительные мощности используются для получения криптовалюты. За год количество инцидентов, связанных с майнингом, выросло на Урале на 40%», – отметил ***Владимир Дрюков, директор центра мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком».***

Еще 32% инцидентов в регионе связано с использованием уязвимостей в веб-приложениях (веб-порталах, электронной почте, интернет-банках, личных кабинетах и т.д.). В целом по стране популярность этого метода выросла на 13%. Как указывают эксперты Solar JSOC, поводом к увеличению числа атак на веб-приложения служит развитие цифровых порталов и внешних ресурсов в компаниях. Помимо традиционных отраслей – банки и ритейл – все

больше веб-ресурсов появляется в энергетике и госсекторе, но при этом каждый третий интернет-сайт имеет критическую уязвимость, позволяющую получить привилегированный доступ к серверу.

На третьем месте в арсенале преступников, атаковавших регион в 2019 году, оказался метод подбора и компрометации учетных данных (логинов и паролей) от интернет-ресурсов организаций. Данный инструмент применялся в 19,6% случаев. Среди прочих типов кибератак, осуществлявшихся на компании Уральского федерального округа, эксперты Solar JSOC выделяют попытки компрометации логинов и паролей системных администраторов, DDoS (атаки, приводящие к недоступности веб-сайтов) и эксплуатацию известных уязвимостей, которые не были своевременно устранены службами информационной безопасности организаций.

Статистика кибератак в Центральном федеральном округе

За 2019 год центр мониторинга и реагирования на киберугрозы Solar JSOC компании «Ростелеком» выявил и отразил свыше 1,1 млн внешних атак на информационные ресурсы организаций. При этом традиционно наибольшее число инцидентов такого рода – более 430 тысяч – было выявлено в Москве. В Центральном федеральном округе за год было зафиксировано свыше 83 тысяч атак.

Большая часть атак в регионе (35%) была реализована с помощью вредоносного ПО (вирусов, троянов, шпионского ПО и т.п.). Как отмечают эксперты Solar JSOC, этим инструментарием хакеры пользуются все активнее – в 2019 году количество инцидентов с применением вредоносов выросло на 11%, причем преступники постоянно их совершенствуют, делая все менее заметными для средств защиты.

Вторым по популярности методом взлома инфраструктуры организаций в ЦФО стало использование уязвимостей в веб-приложениях (веб-порталах, электронной почте, интернет-банках, личных кабинетах и т.д.). На эти виды атак приходится 30% всех инцидентов. На третьем месте – подбор и компрометация учетных данных (логинов и паролей) от интернет-ресурсов организаций (21%).

«В Центральном округе фиксируется самый высокий процент успешных brute force – атак с помощью автоматизированного полного перебора паролей к учетным записям – и получения доступа к внешним сервисам организаций. Причины этого – невысокий уровень безопасности информационной инфраструктуры и игнорирование правил парольной политики, таких как сложность и частота смены паролей», – отметил ***Владимир Дрюков, директор центра мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком».***

Среди прочих типов кибератак, осуществлявшихся на компании Центрального федерального округа, эксперты Solar JSOC выделяют попытки компрометации логинов и паролей системных администраторов, DDoS (атаки, приводящие к недоступности веб-сайтов) и эксплуатацию известных уязвимостей, которые не были своевременно устранены службами информационной безопасности организаций.

Статистика кибератак в Южном федеральном округе

За 2019 год центр мониторинга и реагирования на киберугрозы Solar JSOC компании «Ростелеком» выявил и отразил свыше 1,1 млн внешних атак на информационные ресурсы организаций. При этом традиционно наибольшее число инцидентов такого рода – более 430 тысяч – было выявлено в Москве. В Южном федеральном округе за год было зафиксировано свыше 60 тысяч кибератак.

Чуть больше трети (36%) всех инцидентов на юге России связано с распространением вредоносного ПО (вирусы, трояны, шпионское ПО и т.п.). Как отмечают эксперты Solar JSOC, этим инструментарием хакеры пользуются все активнее – в 2019 году количество инцидентов с использованием вредоносов выросло на 11%. Этому способствует развитие почтового фишинга как основного способа доставки вредоносного ПО.

«В регионе мы отмечаем самый высокий процент заражения вирусным ПО через почтовые рассылки. При этом местные организации, как правило, укомплектованы только базовыми средствами защиты, которые не имеют возможности выявлять не детектируемый антивирусом вредоносный софт», – отметил ***Владимир Дрюков, директор центра мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком».***

Вторым по популярности методом взлома инфраструктуры организаций региона стала эксплуатация уязвимостей веб-приложений (веб-порталов, электронной почты, интернет-банков, личных кабинетов и т.д.). Этот вариант злоумышленники использовали в 29% случаях. На третьем месте – подбор и компрометация учетных данных (логинов и паролей) от интернет-ресурсов организаций – 20% инцидентов.

Среди прочих типов кибератак, осуществлявшихся на компании Южного федерального округа, эксперты Solar JSOC выделяют попытки компрометации логинов и паролей системных администраторов, DDoS (атаки, приводящие к недоступности веб-сайтов) и эксплуатацию известных уязвимостей, которые не были своевременно устранены службами информационной безопасности организаций.