

Отчет о проблемах информационной безопасности в ИТ-инфраструктурах государственных организаций

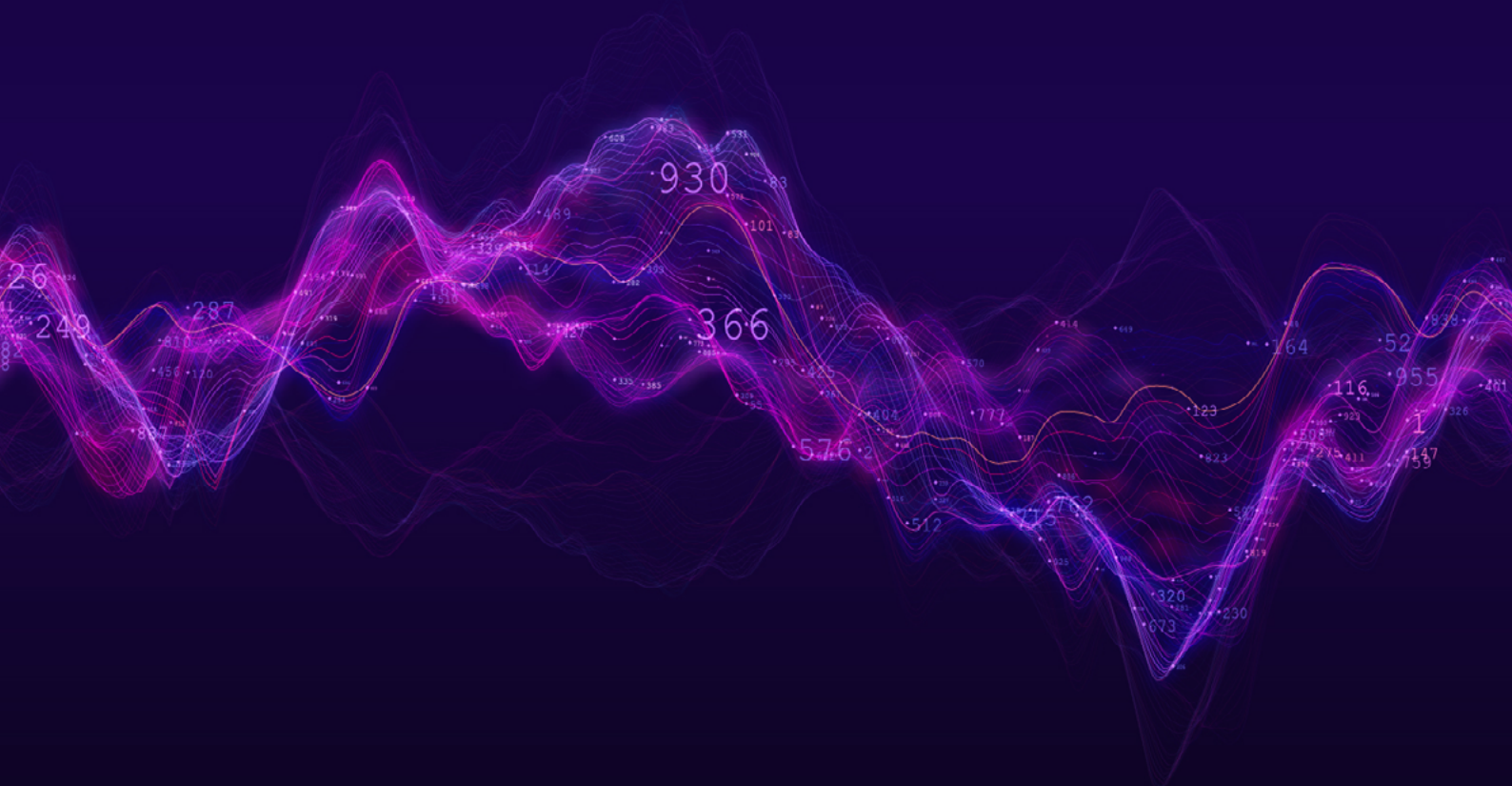
— ПЕРВОЕ ПОЛУГОДИЕ 2020 ГОДА

Открытая часть исследования



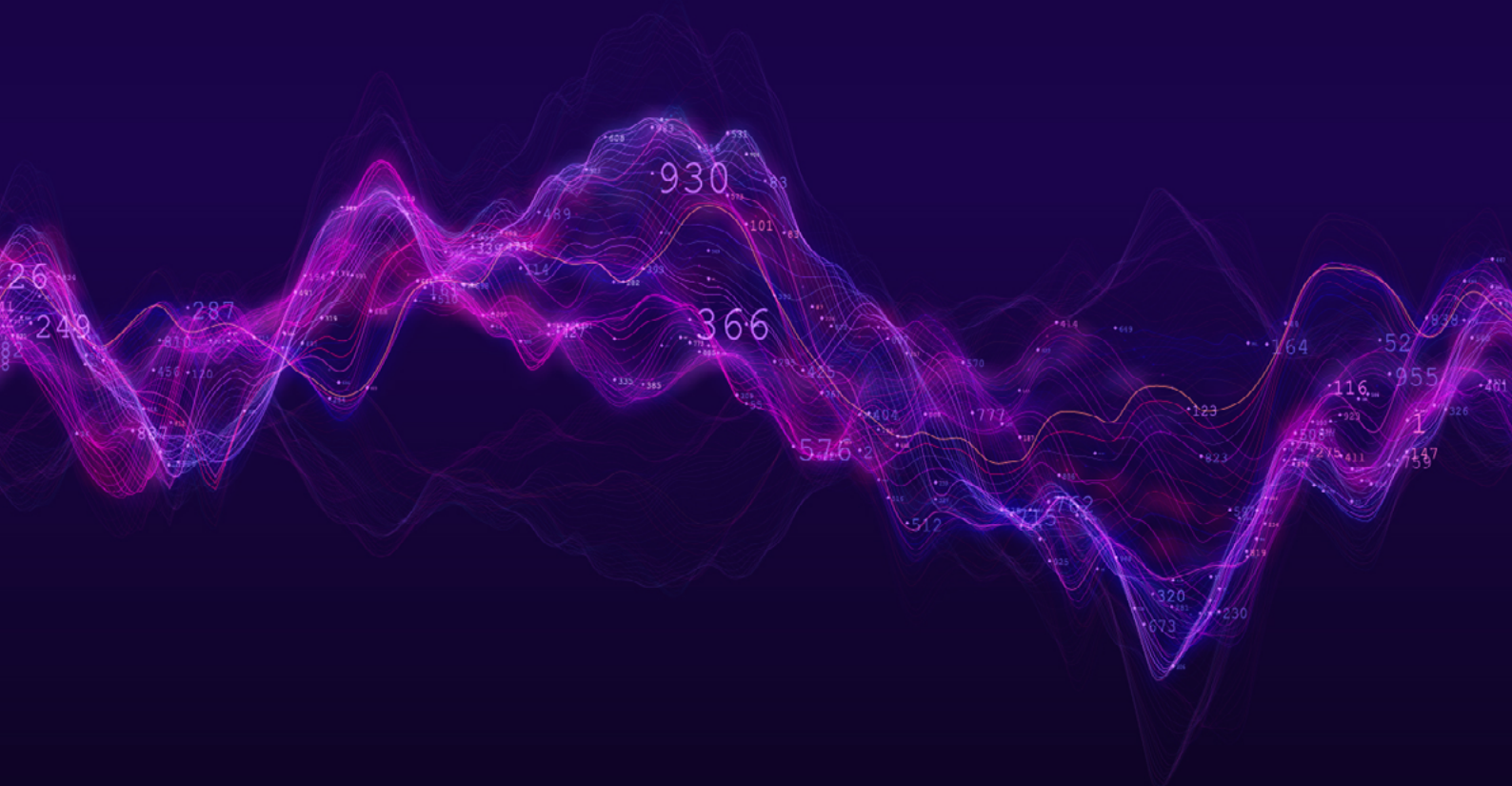
Оглавление

ВВЕДЕНИЕ.....	3
КАК МЫ СЧИТАЛИ?	4
КТО АТАКУЕТ ГОСОРГАНЫ?	5
КАК КИБЕРХУЛИГАНЫ АТАКУЮТ ГОСОРГАНЫ?.....	6
КАК АТАКУЮТ КИБЕРНАЕМНИКИ И КИБЕРВОЙСКА?.....	12
ЗАКЛЮЧЕНИЕ	16



Введение

Органы власти и госорганизации представляют особый интерес для злоумышленников. С одной стороны, их информационные системы хранят множество конфиденциальной и персональной информации, с другой – атаки на этот сегмент несут серьезные репутационные риски и вызывают широкий общественный резонанс. В рамках отчета мы сформировали портрет потенциального злоумышленника, который опасен именно для госсектора, а также составили перечень самых распространенных уязвимостей, которые эксперты центра мониторинга и реагирования на кибератаки Solar JSOC выявили в первом полугодии 2020 года.



Как мы считали?

В рамках исследования эксперты Solar JSOC проанализировали данные о более чем 40 государственных организациях федерального и регионального уровня. В выборку включены, в частности, органы власти и медицинские организации.

Многие уязвимости, представленные в отчете, были обнаружены на этапе проведения пилотных проектов с заказчиками или при их подключении к сервисам мониторинга и реагирования на атаки (все уязвимости впоследствии были устранены совместно с ИБ-службами заказчиков). Часть ошибок в настройке систем безопасности удалось выявить в ходе работ по реагированию или расследованию сложных компьютерных инцидентов, выполняемых специалистами центра расследования киберинцидентов JSOC CERT, а также работ по анализу защищенности, тестированию на проникновение или Red Teaming, выполняемых специалистами Solar JSOC.

В данном отчете мы выделили фундаментальные проблемы информационной безопасности в ИТ-системах госструктур. В область исследования не включены изменения инфраструктуры, связанные с пандемией и переходом на удаленный режим работы, так как они носят стихийный характер и не отражают ключевые векторы развития ИТ- и ИБ-ландшафтов в данном сегменте.



Кто атакует госорганы?

Последнее время эксперты Solar JSOC отмечают существенную сегментацию профиля киберпреступников.

Как правило, атаки на госсектор инициируются либо так называемыми базовыми злоумышленниками с простым инструментарием, либо кибергруппировками, которые применяют более сложные методики и специально разработанные хакерские утилиты.



КИБЕРХУЛИГАНЫ

Они эксплуатируют системные проблемы в инфраструктуре государственных организаций, а их цель – несложная монетизация. Они занимаются шифрованием серверов и рабочих станций, майнингом криптовалюты, созданием из полученных ресурсов бот-сетей для организации DDoS-атак или фишинговых рассылок, а также перепродажей полученных доступов более профессиональным хакерам.



КИБЕРНАЕМНИКИ И КИБЕРВОЙСКА

Они не брезгают результатами деятельности предыдущих группировок для получения первого проникновения в инфраструктуру, а дальше стараются продвигаться по ней максимально незаметно, получая длительный контроль и доступ к конфиденциальным данным (кибершпионаж).

Как киберхулиганы атакуют госорганы?

Ниже представлены распространенные уязвимости и векторы атак, обнаруженные за отчетный период и используемые киберпреступниками со средним уровнем квалификации и несложным инструментарием.

ОТСУТСТВИЕ ОБНОВЛЕНИЯ СЕРВЕРОВ И РАБОЧИХ СТАНЦИЙ В ИЗОЛИРОВАННЫХ СЕГМЕНТАХ СЕТИ

Уровень кибергигиены в части установки обновлений в России и мире крайне низкий: в самой продвинутой, кредитно-финансовой, сфере время установки обновлений занимает **от 42 дней**. Если серверы или компьютеры сотрудников имеют доступ в интернет, есть вероятность, что служба обновления сама «подтянет» необходимые пакеты. Но в случае с госсектором ситуация усугубляется формированием закрытых и изолированных сегментов, не подключенных к глобальной сети. В этом случае необходим формализованный ручной или полуручной процесс по обновлению, который отсутствует в **96% организаций**.

В 96%

организаций
отсутствует ручной
или полуручной
процесс по
обновлению ПО

ИЗ-ЗА ТОГО, ЧТО ИНФРАСТРУКТУРА ОСТАЕТСЯ БЕЗ ОБНОВЛЕНИЯ ДОЛГИЕ ГОДЫ, ФОРМИРУЮТСЯ СЕРЬЕЗНЫЕ СИСТЕМНЫЕ УЯЗВИМОСТИ:

более 90% рабочих станций и серверов уязвимы перед **BlueKeep** и **DejaBlue**. Они позволяют мгновенно распространить вирус-червь или шифровальщик через ошибки в реализации протокола RDP (протокол удаленного рабочего стола);

более 70% рабочих станций и серверов уязвимы перед **EternalBlue** (эксплуатирует ошибки Windows-реализации протокола SMB, который нужен для удаленного доступа к файлам, принтерам и другим сетевым ресурсам). Это привело к массовому распространению печально известных вирусов **WannaCry** и **NotPetya** в 2017 году;

в каждой организации выявляется **не менее 5** рабочих станций, уязвимых перед **MS08-067**, которая была устранена в обновлениях более 12 лет назад. Ошибка позволяет удаленно выполнить произвольный код в контексте службы «Server» (обеспечивает поддержку удаленного вызова процедур), в результате чего злоумышленник может получить дистанционный контроль над всей системой.



ИСПОЛЬЗОВАНИЕ УНАСЛЕДОВАННЫХ (LEGACY) ИНФОРМАЦИОННЫХ СИСТЕМ С УСТАРЕВШИМ КОДОМ И ПРИНЦИПАМИ РЕАЛИЗАЦИИ ПРОТОКОЛОВ БЕЗОПАСНОСТИ

На этапе создания системы ее разработчики зачастую закладывают все необходимые требования по обеспечению безопасности и корректности процессов обновления основных компонентов. Но со временем поддержка отдельных компонентов прекращается и они становятся legacy (т.е. «унаследованными»), что при их взаимодействии с инфраструктурными компонентами (ОС, СУБД, частные приложения) накладывает ограничения на возможности их обновления, поскольку система может целиком выйти из строя. Нередко системы могут опираться на версии ОС, снятые с поддержки более 5 лет назад.

Кроме того, информационные системы, разрабатываемые для госсектора, требуют возможности пользовательского или клиентского доступа, а также часто должны быть связаны с системами других ведомств.



НА ИТ-ПЕРИМЕТРЕ ГОССТРУКТУР МЫ ВИДИМ ОПУБЛИКОВАННЫЕ СИСТЕМЫ И ВЕБ-ПРИЛОЖЕНИЯ СО СЛЕДУЮЩИМИ ФУНДАМЕНТАЛЬНЫМИ ПРОБЛЕМАМИ:

более 50% организаций используют незащищенное соединение (чаще всего это протокол http, в котором передаваемые данные не шифруются и могут быть перехвачены);

более 70% организаций подвержены классическим web-уязвимостям, которые злоумышленники используют в качестве точки входа в инфраструктуру жертвы. Например, подверженность SQL-инъекциям, которые позволяют взломать базу данных сайта и внести изменения в скрипт. Или уязвимости XSS, с помощью которой злоумышленник может интегрировать в страницу сайта-жертвы собственный скрипт;

более 60% организаций имеют уязвимости различных компонентов (серверов Apache или решений для запуска веб-приложений Apache Tomcat, систем управления сайтом WordPress, языка программирования PHP) и даже самой операционной системы (серия уязвимостей Shellshock, которые считаются одними из наиболее опасных).

Особенность реализации данных уязвимостей такова, что позволяет взломать инфраструктуру и получить привилегированный доступ к ней даже без ручного участия злоумышленника, а только с помощью специализированных автоматизированных систем.





ОТСУТСТВИЕ БАЗОВОЙ ЗАЩИТЫ ЭЛЕКТРОННОЙ ПОЧТЫ

В большинстве (**более 70%**) государственных организаций отсутствуют специализированные средства для фильтрации входящей электронной почты. Часто не установлены даже базовые инструменты – антиспам и антивирус.

Это позволяет злоумышленникам напрямую присылать сотруднику исполняемый файл, даже не маскируя вредоносное тело. В итоге для подобных атак используется самое примитивное вредоносное ПО, которое распространяется в даркнете бесплатно. А общий низкий уровень осведомленности пользователей в вопросах кибергигиены гарантирует практически 100%-й успех даже самой простой фишинговой рассылки.



В ИТОГЕ

При проведении расследований, подключении заказчиков, а также в рамках собираемой аналитики мы наблюдаем картину, при которой большинство государственных организаций заражены хорошо известным и относительно старым ВПО, которое входит в арсенал злоумышленников с низкой квалификацией:

85%

поражены
семействами вирусов
DbgBot, Mirai,
Monero Mine

60%

имеют в своей
инфраструктуре
признаки ВПО
WannaCry, WannaMine

55%

поражены
червем Conficker,
эксплуатирующим
уязвимость MS08-067

90%

имеют признаки
ВПО типа червь,
переносимого через
внешние носители

Как атакуют кибернаемники и кибервойска?

Если же базовые уязвимости устранены, это еще не гарантирует полную защиту организации, так как самостоятельно обезопасить себя от злоумышленников высокого уровня они чаще всего не могут.

НЕДОСТАТОЧНАЯ ПРОРАБОТКА СЕТЕВОЙ АРХИТЕКТУРЫ И КОНТУРОВ БЕЗОПАСНОСТИ ПРИ ВНЕДРЕНИИ НОВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

При внедрении новой информационной системы в государственных структурах крайне редко проводится анализ состояния текущей инфраструктуры (сегменты, доступы, маршрутизация). В итоге появляются лишние точки входа в систему – например, через VPN из соседнего ФОИВа.

В 80%

случаев
происходит
«склеивание»
различных
сегментов сети

Также в 80% случаев происходит «склеивание» различных сегментов сети для обеспечения работоспособности вновь создаваемой системы (например, соединение сегмента DMZ, содержащего общедоступные сервисы, и изолированного сегмента Database). В результате злоумышленник легко получает доступ к слабо защищенному элементу инфраструктуры и дальше практически беспрепятственно попадает к критическим информационным активам.



ОТСУТСТВИЕ ПОЛНОЦЕННОГО ПРОЦЕССА ИНВЕНТАРИЗАЦИИ АКТИВОВ И КОНТРОЛЯ СЕТЕВОГО ДОСТУПА

На фоне указанной выше проблемы складывается ситуация, при которой между сегментами сети разрешено гораздо больше, чем необходимо (например, полный доступ через временное «потерянное» оборудование из сегмента DMZ в закрытый сегмент). Или же в инфраструктуре остается «забытое» оборудование, которое когда-то использовалось для построения временной информационной системы с минимальными средствами защиты.

В итоге **90% госорганизаций** имеют от 3 до 10 точек связанности публичного и закрытого сегментов, что может использоваться злоумышленниками для атаки или получения доступа к конфиденциальной информации.





БОЛЬШОЕ КОЛИЧЕСТВО БЫСТРО МЕНЯЮЩИХСЯ ПОДРЯДНЫХ ОРГАНИЗАЦИЙ

В государственных организациях работы по созданию информационных систем или обслуживанию существующей инфраструктуры выполняют, как правило, внешние подрядчики, которые при этом часто меняются в силу контрактных обязательств и ограничений договорных отношений. Это влечет за собой череду опасных модификаций инфраструктуры.

Во-первых, в госорганизациях (как и во многих других отраслях) обычно отсутствует единая точка входа для подрядных организаций, которые работают дистанционно (Jump Server – самый простой вариант организации точки входа). Каждый подрядчик использует свой способ: VPN, Remote Desktop, Remote Admin Tools. Когда контракт с обслуживающей организацией заканчивается, возможность удаленного доступа через ранее используемый канал может сохраняться еще долгое время.

Это способно привести как к заражению трояном удаленного доступа (RAT), который позволяет хакерам отслеживать и контролировать конкретный компьютер или всю сеть, так и к компрометации логинов и паролей.

Во-вторых, хакеры могут атаковать самого подрядчика. Это проблема Trusted Relationship, то есть установления доверительных отношений и высокого уровня привилегий для компаний, априори имеющих низкий уровень обеспечения информационной безопасности. Кража пароля, заражение машины подрядчика или компрометация статического канала связи между инфраструктурами позволяют злоумышленникам, используя технику supply chain (то есть атака через подрядчика), развивать атаку на организацию.

Усугубляется этот процесс высоким уровнем прав и привилегий сотрудников подрядных компаний в ключевых системах инфраструктуры госорганизации. Зачастую для корректной работы подрядчикам требуются административные привилегии. Но даже после окончания контракта их учетные данные остаются активными. Так, в группе Domain Admins (администраторы домена) мы встречаем **от 10 до 30 учетных записей**, 5 из которых использовались больше года назад, но оставались активными.

В ИТОГЕ

Некорректный процесс работы с подрядчиками является одной из наиболее критических уязвимостей органов государственной власти и требует пристального процессного и технического контроля.

Отсюда можно сделать вывод, что профессиональные злоумышленники используют в первую очередь не технические, а процессные уязвимости, связанные с недостаточностью корректной организации и обеспечения работ в части информационной безопасности.

Заключение

Инфраструктуры органов государственной власти и госорганизаций имеют множество уязвимостей и архитектурных ошибок, которые используют киберпреступники. При этом атаки на госсектор инициируются либо так называемыми киберхулиганами с простым инструментарием, либо кибернаемниками и кибервойсками с более сложными методиками.

Массовые проблемы связаны с отсутствием своевременного обновления ПО, использованием устаревших версий программ и отказом от базовых средств защиты.

- Ошибки в реализации протокола **удаленного рабочего стола (RDP)** имеют более 90% рабочих станций и серверов.
- Ошибки в реализации протокола **удаленного доступа к сетевым ресурсам (SMB)** – в более 70% организаций.
- **Незащищенное интернет-соединение** используют более 50% организаций.
- Нет **базовых средств защиты** электронной почты – в 70% организаций.
- **Уязвимости веб-приложений** – в 70% организаций.

К проблемам, которые позволяют проводить более сложные атаки, относятся **«склеивание» публичного и закрытого сегментов сети** (в 90% организаций) и **появление неучтенных точек доступа** к системе. Достаточно распространенной для госорганов является **атака через подрядчика**.



О компании

«Ростелеком-Солар», компания группы ПАО «Ростелеком», — национальный провайдер сервисов и технологий для защиты информационных активов, целевого мониторинга и управления информационной безопасностью.

В основе подходов и технологий «Ростелеком-Солар» лежит понимание, что настоящая информационная безопасность возможна только через непрерывный мониторинг и удобное управление системами защиты.



Задать вопрос или
попробовать сервис
info@rt-solar.ru

