[Из кода в код]

Если говорить о трендах в области кибербезопасности, которые стоит ожидать в 2024-м, то, по мнению экспертов белорусского представительства Kaspersky, все те угрозы, которые наблюдались в минувшем году, по-прежнему остаются актуальными.

Специалисты компании дополняют, что одну из основных опасностей в мире представляют программы-вымогатели. При этом в Беларуси за первое полугодие 2023 года объем атак с использованием программ-шифровальщиков вырос более чем на 25 % по сравнению с аналогичным периодом предыдущего года. Об этом шел разговор на пресс-конференции накануне ежегодной масштабной конференции по кибербезопасности Kaspersky Security Day 2023, состоявшейся в Большом театре Беларуси. Мероприятие собрало участников со всех регионов страны: менеджеров высшего звена, представителей государственных структур, экспертов, руководителей и специалистов из ИТ и информационной безопасности.

Эксперты компании обрисовали текущий ландшафт киберугроз для бизнеса и промышленных предприятий, разобрали современные тренды в области информационной безопасности и шаги по построению эффективного центра мониторинга безопасности (SOC). Особое внимание участники уделили тонкостям указа от 14 февраля 2023 года № 40 «О кибербезопасности». Спикерами была предоставлена исчерпывающая информация и необходимые инструменты для его соблюдения.

По мнению специалистов, среди всего разнообразия киберугроз есть те, которые одинаково опасны как для бизнеса, так и для пользователей. К примеру, с января по октябрь 2023 года почти каждый второй (41 %) пользователь из Беларуси столкнулся с локальными киберугрозами*. Речь идет о вредоносных файлах, распространяющихся, например, через съемные носители, в виде зашифрованных документов или в составе сложных инсталляторов. При этом доля корпоративных пользователей, на устройствах которых были зафиксированы попытки заражения локальными угрозами, держится на том же уровне и составляет 39 %.

– Ландшафт киберугроз постоянно усложняется, и сейчас вопросы цифровой безопасности касаются каждого. Организации всегда должны быть на шаг впереди злоумышленников, чтобы оставаться уверенными в сохранении целостности данных. Мы верим, что эффективно противостоять современным кибер-

угрозам можно только сообща: обсуждать проблемы кибербезопасности со всеми заинтересованными сторонами, совместно находить пути решения с опорой на экспертизу и опыт компаний, которые имеют многолетний опыт в области информационной безопасности. Конференция Kaspersky Security Day 2023 – это возможность объединиться и выстроить эффективные стратегии защиты от киберугроз, соответствующие актуальным запросам бизнеса и государства, – комментирует обстановку Дмитрий Кудревич, представитель Kaspersky в Беларуси.

По мнению экспертов, первенство среди пяти наиболее активных преступных кибергруппировок удерживала LockBit. При этом вердикт Trojan-Ransom.Win32.LockBit затронул и белорусские организации, в связи с чем весной минувшего года в Беларуси наблюдался всплеск таких атак. Речь идет об известном вредоносном ПО, чей билдер (шаблон для создания вредоноса) стал доступен широкому кругу пользователей еще осенью 2022-го. С тех пор несколько разных группировок используют этого шифровальщика для проведения своих атак. Среди примеров таких групп можно отметить Shadow и Twelve.

– Количество вредоносных программ может увеличиваться в одних регионах и уменьшаться в других. Однако независимо от динамики, атаки по всему миру становятся более изощренными и целенаправленными. Использование комплексного подхода к киберзащите организации позволит свести к минимуму последствия, возникающие в результате атак вымогательских групп. Защитные решения – необходимая инвестиция, поскольку атаки программ-вымогателей могут привести к необратимой потере информации, времени, финансовых ресурсов, а также нарушению бизнес-процессов, ущербу репутации, – говорит Дмитрий Кудревич.

– Мишенью злоумышленников являются любые организации – от медицинских и образовательных учреждений до поставщиков услуг и промышленных предприятий, – комментирует профильный эксперт Kaspersky Татьяна Шишкова. *– При этом вымогатели продолжают совершенствовать свои методы. Это обуславливается тремя причинами. Первая – высокие шансы попасться при совершении атаки на организацию. Вторая – размер потенциального выкупа. Наконец, хакеры всегда оценивают техническую сложность атаки. Если что-либо из перечисленного выходит за рамки планов злоумышленников, они пересматривают свою тактику,* – объясняет Татьяна Шишкова.

Для борьбы с программами-вымогателями и оказания помощи пострадавшим от них Национальное подразделение высокотехнологичных преступлений полиции Нидерландов, Европейский центр по вопросам киберпреступности Европола, Kaspersky и другие партнеры совместно запустили инициативу No More Ransom в 2016 году. На официальном сайте участники предоставляют дешифратор и рекомендации для жертв подобных атак.

* Анонимизированные данные получены на основе срабатывания защитных компонентов решений Kaspersky за январь – октябрь 2023 года.

г. Минск

ЧТОБЫ ЗАЩИТИТЬ СЕБЯ И БИЗНЕС ОТ АТАК ПРОГРАММ-ВЫМОГАТЕЛЕЙ, KASPERSKY РЕКОМЕНДУЕТ:

- Не подключать службы удаленного рабочего стола (такие как RDP, MSSQL и т. д.) к общедоступным сетям без крайней необходимости, а также всегда использовать надежные пароли, двухфакторную аутентификацию и правила брандмауэра.
- Своевременно обновлять программы и операционную систему на всех устройствах, чтобы предотвратить использование уязвимостей программами-вымогателями.
- Обращать внимание на боковые перемещения в инфраструктуре, а также на исходящий трафик – это поможет обнаружить несанкционированное подключение злоумышленников к вашей сети.
- Настроить автоматическое создание резервных копий и убедиться, что вы можете оперативно получить доступ к своим данным при необходимости.
- Избегать установки приложений из ненадежных источников.
- Провести аудит систем информационной безопасности, которые связаны с партнерами и подрядчиками, а также доступов управляемых служб к вашей инфраструктуре.
- Подготовить план действий на случай кражи и утечки персональных данных.
- Использовать защитные решения, такие как Kaspersky Endpoint Detection and Response Expert и Kaspersky Managed Detection and Response, которые помогут обнаружить атаки и препятствовать им прежде, чем злоумышленники достигнут своей цели.
- Обучать сотрудников основам цифровой грамотности для обеспечения кибербезопасной корпоративной среды. Существуют специальные тренинги, которые помогут в этом – например, Kaspersky Automated Security Awareness Platform.
- Использовать надежное решение для обеспечения безопасности конечных точек – например, Kaspersky Endpoint Security for Business (KESB), которое обеспечивает защиту от эксплойтов, выявляет уязвимости и позволяет выполнять откат действий вредоносной программы. У KESB также есть механизм самозащиты, предотвращающий выполнение другими программами действий, которые могут нарушить работу Kaspersky Endpoint Security и, например, попытаться удалить его с компьютера. KESB также продемонстрировали стопроцентную защиту от программ-вымогателей в ходе тестирования Advanced Threat Protection Test лабораторией AV-TEST. В ходе 10 различных атак продукт не позволил зашифровать ни один из пользовательских файлов.
- Использовать результаты последних исследований, чтобы оставаться в курсе методов, тактик и инструментов злоумышленников. Kaspersky Threat Intelligence Portal предоставляет все знания Kaspersky о киберугрозах, безопасных объектах и связях между ними, собранные командой за более чем 25 лет.