Kaspersky ICS CERT

kaspersky

Киберугрозы для АСУ и промышленных предприятий в 2023 году

Евгений Гончаров

22.11.2022 Version 1.0

Уходящий 2022 год был богат на события кибербезопасности. Он поставил много проблем перед владельцами и операторами промышленных инфраструктур. Однако никаких резких и катастрофических изменений ландшафта угроз, с которыми было бы трудно справиться, мы, к счастью, не увидели, несмотря на большое количество громких заголовков новостных изданий на эту тему.

На наш взгляд, год грядущий сможет стать во многом более сложным. И многих он, вероятно, удивит неожиданными поворотами, рассматривать возможности которых нужно уже сейчас. Мы постарались предугадать некоторые из них, не претендуя, конечно же, ни на полноту, ни на высокую точность предсказаний.

Анализируя события уходящего 2022 года, приходится признать, что мы вступили в эпоху, когда наиболее значимые изменения в ландшафте угроз для промышленных предприятий и OT-инфраструктур будут определяться, прежде всего, геополитическими и связанными с ними макроэкономическими факторами.

Киберкриминал космополитичен по своей природе, но из соображений собственной безопасности и в погоне за лёгкой наживой он будет пристально следить за политическими и экономическими изменениями и чутко реагировать на них.

Активности APT, которые традиционно принято связывать с деятельностью спецслужб различных государств, всегда лежат в фарватерах внешнеполитических интересов государств и согласуются с целями внутри- и межгосударственных блоков.

Направления активности APT

Происходящие внутри- и внешнеполитические изменения, соответственно, зададут **новые направления активности APT**.

Изменения географии атак

Переформатирование существующих и создание новых тактических и стратегических альянсов, свидетелями чего нам всем выпало быть, неминуемо вызовут **изменения и в географии атак**. Напряжённость в сфере кибербезопасности может возникнуть между странами, между которыми её раньше не существовало. И вчерашние «союзники» могут стать новыми целями атак друг для друга.

Смещение отраслевого фокуса

Поскольку геополитическое переформатирование мира обусловлено и неразрывно связано с экономическими изменениями, в скором будущем мы увидим и **смещение отраслевого фокуса активности APT**. В числе мишеней атак всё чаще будут встречаться организации из следующих «реальных» секторов экономики:

- Сельское хозяйство, производство удобрений, сельхозтехники и продуктов питания — ввиду маячащих продовольственных кризисов и переделов продовольственных рынков;
- Логистика и транспорт (включая транспорт энергоресурсов) — ввиду начавшихся глобальных перестроений логистических цепочек;
- Энергетика, добыча и обработка полезных ископаемых, цветная и чёрная металлургия, химическая промышленность, судостроение, приборо- и станкостроение — поскольку доступность продукции этих компаний и их технологий входят в фундамент экономической безопасности стран и политических альянсов;
- Альтернативная энергетика — там, где она продвигается по геополитической повестке;
- Хайтек-компании, фармацевтика и производство медицинского оборудования — поскольку они необходимы для обеспечения технологической независимости.

Продолжение атак на традиционные цели

Разумеется, в активности APT будет прослеживаться и **традиционный** уже **фокус**. Среди основных целей APT будут, безусловно, присутствовать:

- предприятия ВПК (главные факторы активности атакующих — геополитическая напряжённость, переход конфронтаций к «горячей» фазе, рост вероятности военных конфликтов),
- госучреждения — атаки для сбора всевозможного рода информации об инициативах и проектах государства, связанных с развитием промышленных секторов экономики,
- критическая инфраструктура — атаки с целью закрепиться на «чёрный день», а в некоторых случаях (например, при наличии конфликта между государствами «в горячей фазе»), возможно, и с целью нанесения прямого ущерба.

Другие изменения ландшафта угроз

К прочим важным изменениям ландшафта угроз, которые мы уже наблюдаем, и вклад которых в общую картину, вероятно, лишь только увеличится в будущем, стоит отнести следующие:

- Вероятно, вырастет количество хактивистов («работающих» по внутри- и внешнеполитической повестке), и результативность их атак — количество начнёт переходить в качество.
- Увеличится риск появления добровольных идеологически и политически мотивированных инсайдеров, и инсайдеров, включённых в схемы действия криминальных групп (прежде всего, вымогателей) и APT, — как на самих предприятиях, так и среди разработчиков и поставщиков технологий.
- Увеличится вероятность атак вымогателей на критическую инфраструктуру — под «прикрытием» недружественно настроенного государства или в странах, не способных эффективно ответить на атаку злоумышленников атакой на их инфраструктуру и довести расследование до суда.
- Деградация коммуникаций между правоохранительными органами разных стран, остановка программ международной кооперации развязывает руки киберкриминалу — позволяет безопасно «работать» по целям, находящимся в «недружественных странах». Это применимо для всех типов киберкриминальных угроз, актуально для всех предприятий всех промышленных секторов и всех типов OT-инфраструктур.

- Рост спроса на первоначальный доступ к организациям стимулирует криминальные кампании, нацеленные на кражу учетных данных сотрудников.

Факторы риска, обусловленные геополитическими изменениями

Сложившаяся ситуация ставит в условия крайне сложного выбора промышленные организации — продукты каких разработчиков использовать и почему?

С одной стороны, **рвущиеся отношения доверия** в цепочках поставки продуктов и сервисов (включая OEM) увеличивает риски использования многих ставших привычными продуктов:

- Окончание поддержки продуктов или уход вендоров с рынка приводят к проблемам с обновлениями безопасности.
- Точно так же в отсутствие регулярных обновлений происходит качественная деградация уходящих с рынков решений по безопасности.
- Не исключена полностью и возможность применения «политического рычага» в отношении продуктов, технологий и услуг некоторых мелких и средних игроков рынка — для использования их «не по назначению», в том числе и в атаках на объекты промышленной инфраструктуры. Однако, по нашему мнению, вероятность того, что это затронет лидеров рынка и авторитетных производителей, крайне мала.

С другой стороны, поиск альтернативы может оказаться крайне непростым занятием. «Отечественные продукты» от локальных разработчиков, чья **культура безопасной разработки**, как показывает опыт, обычно сильно уступает принятой у мировых лидеров, ожидаемо содержат «глупые» ошибки конфигурации и лёгкие **уязвимости нулевого дня**, доступные и киберкриминалу, и хактивистам.

Организациям в странах, где политическая обстановка не заставляет пока, как будто, задумываться над упомянутой выше проблемой, стоит учитывать **факторы риска, общие для всех**:

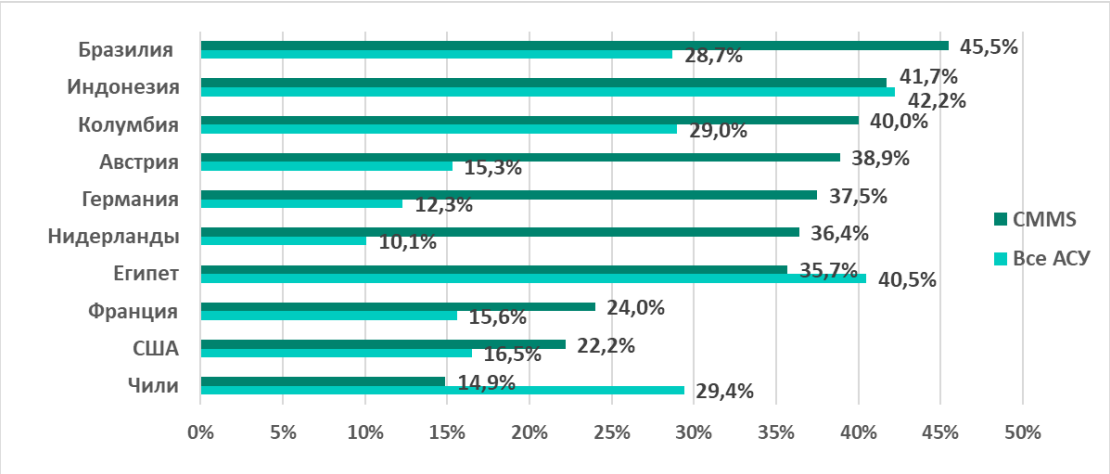
- Потеря части рынков для разработчиков средств ИБ и обычно связанная с ней потеря части квалифицированных экспертов бьют по качеству обнаружения угроз — актуально для всех производителей средств безопасности, находящихся под политическим давлением.

- Рвущиеся коммуникации между исследователями и разработчиками средств ИБ, находящимися по разные стороны нового «железного занавеса» и по одну сторону от него (из-за увеличения конкуренции на локальных рынках), — не могут не сказаться на ухудшении детектирования разрабатываемых средств защиты.
- Ухудшение качества CTI — необоснованная политически мотивированная атрибуция, сгущение красок, общее снижение требований к обоснованности утверждений — под политическим гнётом и в попытке оседлать для получения дополнительной прибыли политические нарративы продвигаемой государством повестки дня.
- Попытки государств консолидировать у себя информацию об инцидентах, угрозах и уязвимостях и ввести дополнительные ограничения на доступ к ней, с одной стороны, ухудшают общий уровень осведомленности — ведь часть информации может «закрываться» необоснованно. С другой стороны, одновременно повышается и риск утечки конфиденциальной информации (пример: PoC RCE, по ошибке опубликованный в национальной базе данных уязвимостей). Решение этой проблемы требует реализации в государственном секторе масштабных мер по повышению квалификации в области кибербезопасности, чтобы гарантировать ответственное обращение с чувствительной информацией об уязвимостях и угрозах и обеспечить при этом эффективную координацию раскрытия таких сведений.
- Возрастающая роль государства в операционной деятельности промышленных предприятий — подключение к государственным облакам и сервисам, зачастую менее защищённым, чем некоторые из лучших частных облаков и сервисов, ведёт к рискам ИБ.

Дополнительные технические и технологические факторы риска

- «Цифровизация» в погоне за повышением эффективности — IIoT и SmartXXX (в том числе, системы управления техническим обслуживанием и цифровые двойники) — означает существенное увеличение поверхности атаки. Об этом можно судить, например, по статистике атак на компьютеризированные системы управления техническим обслуживанием (CMMS, Computerized Maintenance Management System).

Топ 10 стран по проценту CMMS, атакованных в первом полугодии 2022 года



Показательно, что в топ 10 стран по проценту CMMS, атакованных в первом полугодии 2022 года, вошли и традиционно «благополучные» страны, не попадающие в топ ни по общим показателям процента атакованных компьютеров АСУ в стране, ни по процентам атакованных компьютеров в отдельных индустриях.

- Рост цен на энергоносители и, как следствие, удорожание стоимости «железа», с одной стороны, заставит многих отказаться от планов развёртывания on-premise-инфраструктуры в пользу «облаков» сторонних поставщиков услуг (что чревато дополнительными рисками ИБ), с другой стороны, где-то негативно ударит по бюджетам, выделяемым на IT/OT-безопасность.
- Внедрение различных беспилотных транспортных средств и агрегатов (грузовики, дроны, сельхозтехника и прочее), которые сами по себе могут стать как объектом, так и средством реализации атаки.

Наиболее востребованные / эффективные техники и тактики будущих атак

Не станем фантазировать по поводу тактик и техник атак, применяемых наиболее продвинутыми атакующими, такими как APT, связанные со спецслужбами ведущих государств, — тут нас могут поджидать любые сюрпризы. Не станем рассуждать и о тактиках и техниках, используемых наиболее многочисленными злоумышленниками из числа наименее квалифицированных — здесь, скорее всего, ничего нового и интересного нас не ждёт, и эффективно противостоять им способны, как правило, уже имеющиеся на большинстве предприятий средства и меры защиты.

Сосредоточимся на техниках и тактиках средней степени сложности, составляющих арсенал наиболее активных APT-групп, действия которых традиционно принято связывать с интересами восточных и ближневосточных стран, а также активно применяемых продвинутыми категориями киберкриминала, такими как вымогатели.

По опыту исследования таких атак и расследования связанных с ними инцидентов, считаем, что наибольшего внимания специалистов по кибербезопасности промышленных предприятий требуют следующие тактики и техники:

- Фишинговые страницы и скрипты, внедрённые на легитимных сайтах.
- Использование протроянненных «поломанных» дистрибутивов, а также «патчей» и генераторов ключей общеупотребимого и специализированного ПО (также подстёгивается увеличением стоимости лицензий и уходом производителей с рынков под политическим давлением).
- Фишинговые письма «на злобу дня» — с наиболее животрепещущими темами, в том числе, связанными с событиями, первопричины которых имеют политические корни.
- Документы, украденные в предыдущих атаках на смежные организации и организации–партнёры, — в качестве «приманки» в фишинговых письмах.
- Распространение фишинговых писем из скомпрометированных почтовых ящиков сотрудников и контрагентов под видом легальной рабочей переписки.
- N-day уязвимости — они теперь ещё медленнее будут закрываться ввиду ухудшения доступности обновлений безопасности некоторых решений.

- Использование глупых ошибок в конфигурации (типа оставленных паролей по умолчанию) и 0-day уязвимостей в продуктах «новых», в том числе и локальных («отечественных») вендоров — массовое внедрение таких продуктов неизбежно, несмотря на серьёзные вопросы к уровню зрелости безопасности разработчиков. Так, например, рекомендации типа «в окне задания пароля установить такой-то пароль» встречаются в инструкциях по установке и эксплуатации удивительно большого процента продуктов небольших «локальных» вендоров, а на сайте производителя вы никогда не найдёте информации об уязвимостях, наследуемых вместе с использованными общими компонентами и OEM-технологиями, а часто и вообще ни о каких уязвимостях в продуктах вендора.
- Использование недостатков безопасности облачных решений от «отечественных» поставщиков сервисов и государственных информационных систем — по той же причине, что и в предыдущем случае.
- Использование ошибок конфигурации средств защиты. Таких как, например, возможность отключить антивирус без ввода пароля администратора (антивирус мало полезен, если злоумышленник может легко его отключить). Второй пример — слабая защита систем централизованного управления средствами ИБ. В таких случаях средства ИБ можно не только легко обойти, но и использовать их для развития атаки — например, для доставки вредоносного ПО или для получения доступа к «изолированным» сегментам сети и обхода правил разграничения доступа.
- Использование популярных облачных сервисов в качестве CnC — даже после обнаружения атаки жертва может оказаться не в состоянии их заблокировать, потому что на их использовании завязаны какие-то важные бизнес-процессы.
- Использование уязвимостей легитимного ПО, например, DLL Hijacking и BYOVD (Bring Your Own Vulnerable Driver) для обхода средств защиты конечных узлов.
- Распространение вредоносного ПО через флэшки для преодоления air gap (там, где он на самом деле есть).

Вместо заключения

При написании прогнозов мы ставили задачу не обрисовать весь набор возможных угроз, а передать ощущение глобальности грядущих изменений и направить мысль читателей в сторону оценки тех из них (или других подобных, но не упомянутых в тексте), которые наиболее релевантны их организации.

В нашем списке мы привели только те изменения и обозначили те риски, которые мы считаем наиболее масштабными и общими для многих организаций из многих стран. Отчасти поэтому некоторые из прогнозов могут показаться общими и не вполне конкретными.

Понять, какие из угроз на самом деле актуальны конкретно для вас, можете только вы сами. Разумеется, если в этом, не таком уж простом, как может показаться на первый взгляд, деле вы рассчитываете на нашу помощь, мы всегда готовы помочь.

Наши прогнозы — сумма мнений наших экспертов, основанных на коллективном опыте исследования уязвимостей, атак и расследования инцидентов, а также на личном видении направления изменения основных движущих факторов ландшафта угроз. Мы будем только рады, если какие-то из негативных предсказаний не сбудутся в 2023 году.

Если у вас возникли вопросы касательно рассуждений, которые легли в основу наших прогнозов, или вы хотели бы обсудить с нами какие-то из них, пишите нам по адресу ics-cert@kaspersky.com, будем рады ответить.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com