В 39% случаев эксперты обнаружили следы активности 17 известных APT-группировок.

Специалисты отдела реагирования на угрозы ИБ экспертного центра безопасности Positive Technologies – это российская компания, специализирующаяся на кибербезопасности. Является одним из ведущих мировых поставщиков услуг и продуктов в этой области.” data-html=”true” data-original-title=”Positive Technologies” >Positive Technologies (PT ESC IR) представили на SOC-форуме статистику по итогам проектов по расследованию киберинцидентов и ретроспективному анализу по итогам года.За последний квартал 2023 года и первые три квартала 2024 года к специалистам чаще всего обращались промышленные предприятия, государственные учреждения и IT-компании. Основными причинами успешных атак были устаревшее программное обеспечение, отсутствие двухфакторной аутентификации и слабая сегментация корпоративной сети.

Согласно отчету, в 39% проанализированных компаний были обнаружены следы активности 17 известных организованных преступных группировок (APT). Эти группы идентифицируются по применяемым инструментам и вредоносному ПО, инфраструктуре и тактикам. Зачастую они используют специализированное программное обеспечение для удаленного доступа, сбора и кражи данных. . Большая часть выявленных группировок имеет высокую квалификацию и способна быстро достигать поставленных целей.

Среди всех группировок, обнаруженных за период исследования, команда PT ESC выделила три: Hellhounds — как одну из самых продвинутых с точки зрения техник, ExCobalt — как самую активную, а XDSpy — как наиболее долгоживущую группу (она атакует компании в России с 2011 года).

Частота атак через подрядчиков увеличилась на 15% за год. Многие из этих подрядчиков оказывают услуги десяткам клиентов. «Несмотря на то, что доля таких атак пока небольшая, реальный и потенциальный ущерб от взлома доверенных, но незащищенных партнеров приобретает лавинообразный характер»,— отмечают в Positive Technologies. Среди методов первоначального проникновения лидирующее место по-прежнему занимает эксплуатация уязвимостей в веб-приложениях. В течение последнего года наибольшее число атак (33%) пришлось на сайты, работающие на CMS «1С-Битрикс», что сделало их основным вектором проникновения через уязвимые веб-приложения. При этом доля атак, начинавшихся с эксплуатации уязвимостей в почтовых серверах Microsoft Exchange, сократилась с 50% до 17%.

В 35% компаний были зафиксированы инциденты, относящиеся к категории

«Cybercrime» — атаки, ориентированные преимущественно на деструктивные действия, такие как шифрование данных и их уничтожение. В таких случаях злоумышленники, как правило, используют шифровальщики, легитимное программное обеспечение для шифрования информации и вайперы для полного удаления данных. Эти инструменты также применяются для сокрытия следов и максимального усложнения процесса расследования инцидента.

По сравнению с предыдущими годами, доля случаев, в которых киберинциденты приводили к сбоям в бизнес-процессах, выросла с 32% до 50%. Причиной этого может быть усиление активности хактивистов и финансово мотивированных злоумышленников. В 19% проектов были выявлены следы разведывательной активности и шпионажа, которые обычно ассоциируются с деятельностью APT-группировок. В 12% случаев злоумышленники пытались выгрузить конфиденциальные данные, при этом избегая длительного нахождения в инфраструктуре компании. Как и ранее, основными целями атак оставались узлы на базе Windows, однако доля атак на узлы под управлением Linux также была значительной (28%).

Эксперты отмечают существенный рост востребованности отечественными компаниями работ по расследованию инцидентов. За последние два года их количество увеличилось в три раза.