

ИССЛЕДОВАНИЕ НЕЗАДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В.В. Маликов

*Совместное открытое акционерное общество «Коммунарка»,
Минск, Беларусь*

В целях выявления возможных незадекларированных возможностей установленного прикладного программного обеспечения и уязвимостей в информационно-управляющей системе производственно-хозяйственной деятельности было проведено исследование уровня информационной безопасности с использованием решений «Kaspersky Symphony XDR».

В результате исследования было выявлено 128 случаев, детектированных компонентами «Kaspersky Symphony XDR» как аномальные (отличные от типовых / разрешенных правил функционирования).

В ходе детального изучения аномальных случаев функционирования были получены результаты:

- по причине генерации значительного числа подозрительных запросов к внешним ресурсам сети интернет – удалены 2 прикладных программных продукта, распространяемых в категориях «GNU» / «Freeware»;

- установлены и устранены попытки эксплуатации уязвимости операционной системы Windows;

- дополнительно установлена защита от нелегитимных задач/установки новых сервисов в планировщиках хостов и обращений к вредоносным ресурсам в сети интернет.

По результатам проведенного исследования принято решение о минимизации использования программных продуктов, распространяемых в категориях «GNU»/«Freeware».