УДК 004.896

ОБЗОР ИНТЕЛЛЕКТУАЛЬНЫХ ВРЕДОНОСНЫХ ПРОГРАММ И ПОДХОДОВ К ИХ ВЫЯВЛЕНИЮ

Хабибуллин А.В., Менисов А.Б. (Военно-космическая академия имени А.Ф.Можайского)
Научный руководитель – к.т.н. Менисов А.Б. (Военно-космическая академия имени А.Ф.Можайского)

Аннотация. В докладе рассмотрена осуществимость интеллектуальных вредоносных программ, которые могут быть использованы в современных атаках на вычислительную инфраструктуру через киберфизическую систему (Cyber-Physical System, CPS). В качестве доказательства смоделирована охлаждающая система центра обработки данных и представлена логика обучающегося вредоносного ПО, которая имитирует сбои и аномальные события.

Введение. Растущая сложность CPS, хотя и обеспечивает новые прорывы в различных областях применения, также создает новые уязвимости, которые могут быть использованы злоумышленниками. В типичной CPS вычислительная инфраструктура обеспечивает поддержку физической инфраструктуры, и отказоустойчивость таких систем привлекает значительное внимание как исследователей, так и практиков. Однако был обнаружен другой недостаточно изученный сценарий, в котором злоумышленник пытается отключить вычислительную инфраструктуру и вызвать общесистемный сбой, скомпрометировав CPS самообучающимся вредоносным ПО.

Основная часть. В модели угроз предполагается:

1. Система управления охлаждением (CPS), которая менее безопасна чем целевая вычислительная инфраструктура, и ее относительно легче использовать;
2. Злоумышленник, который имеет возможность получить удаленный доступ (например, путем фишинга, кражи учетных данных или внутренней атаки), идентифицировать целевой параметр(ы) (например, расход и температура охлажденной воды, подаваемой в серверную);
3. Умное вредоносное ПО с возможностью автоматически выводить стратегии атаки, также имеющее доступ к измерениям CPS и копиям программ программируемых логических контроллеров (ПЛК), хранящиеся на сервере управления в качестве резервной копии.

После внедрения в CPS вредоносное ПО проходят следующие этапы обучения:

1. Идентификация режимов работы – применение кластеризации методом k-средних по двум параметрам: расход охлажденной воды и разница температур между подачей и обработкой водой;
2. Снижение целевых параметров – выбор 10 из 47 параметров с наибольшей корреляцией, также фиксация отношения между критическими параметрами, чтобы свести к минимуму контекстную несогласованность во время внедрения ложных данных;
3. Фильтрация событий с аномальными измерениями с помощью распределения Гауса.

После того, как вредоносная программа определяет аномальные события, производится идентификация контроллера (ПЛК), который использует критические параметры в качестве входных данных. Для идентифицированного ПЛК вредоносное ПО модифицирует программу ПЛК для проверки условий, инициирующих атаку, и перезаписывает нормальные значения критических параметров последовательностью аномальных значений. Вредоносное ПО завершает подготовку атаки, загружая модифицированную программу в ПЛК.

Выводы. В результате исследования были найдены 3 из 5 системных сбоев (сценариев атак), которые были успешно реализованы вредоносным ПО в смоделированной системе CPS с реальными данными.