Темная сторона: как меняются векторы и способы атак злоумышленников

Артем Кильдюшев
Руководитель группы пресейла Solar JSOC
компании «Ростелеком-Солар»

Ростелеком
Солар

Solar JSOC

Solar JSOC – первый и крупнейший в России коммерческий центр мониторинга и реагирования на инциденты кибербезопасности (SOC), действующий по модели MDR (Managed Detection and Response)

№1

на рынке SOC
В России

250+

экспертов
кибербезопасности

140+

клиентов из всех
отраслей экономики

110+

млрд анализируемых
событий ИБ в сутки

Ростелеком
Солар

Что анализировали?

1 Выявленные инциденты у клиентов в рамках сервисов Solar JSOC

2 Инциденты, расследуемые командой Solar JSOC CERT

3 Информация, собранная на honeypot

4 Информация, полученная в рамках информационного обмена

Ростелеком
Солар

Киберландшафт-2020

Рост квалификации злоумышленников

Усложнение инструментария

Повышение темпа использования новых уязвимостей

Длительное присутствие в инфраструктуре

Итог: расслоение подходов злоумышленников к атакам на инфраструктуру

Уровни злоумышленников

	УСЛОВНАЯ КАТЕГОРИЯ НАРУШИТЕЛЯ	ТИПОВЫЕ ЦЕЛИ	ВОЗМОЖНОСТИ НАРУШИТЕЛЯ
1	Автоматизированные системы	Взлом устройств и инфраструктур с низким уровнем защиты для дальнейшей перепродажи или использования в массовых атаках	Автоматизированное сканирование
2	Киберхулиган/ Энтузиаст-одиночка	Хулиганство, нарушение целостности инфраструктуры	Официальные и open-source-инструменты для анализа защищенности
3	Киберкриминал/ Организованные группировки	Приоритетная монетизация атаки – шифрование, майнинг, вывод денежных средств	Кастомизированные инструменты, доступное вредоносное ПО (приобретение, обфускация или разработка), доступные уязвимости, социнжиниринг
4	Киберкаемники/ Продвинутые группировки	Нацеленность на заказные работы – сбор информации, шпионаж в интересах конкурентов, последующая крупная монетизация, хактивизм, деструктивные действия	Самостоятельно разработанные инструменты, приобретенные zero-day-уязвимости ПО
5	Группировки, спонсируемые государствами	Кибершпионаж, полный захват инфраструктуры для возможности контроля и применения любых действий и подходов, хактивизм	Самостоятельно найденные zero-day-уязвимости ПО и АО, разработанные и внедренные "закладки"

Ростелеком
Солар

Статистика по группировкам среднего уровня

Ростелеком
Солар

Статистика по группировкам высокого уровня

Ростелеком
Солар

Основные техники закрепления и распространения

- Механизмы автозагрузки
- Системные службы
- Формирование собственных драйверов
- Использование удаленных сервисов
- Pass the Ticket / Pass the Hash
- Использование WMI для работы ВПО
- Использование ОС для работы инструментария BITS-задач
- Использование планировщика задач
- Эксплуатация уязвимостей удаленных сервисов

Ростелеком
Солар

Техники закрепления

- Системные службы
- Использование BITS-задач
- Формирование собственного драйвера
- Использование планировщика задач
- Механизмы автозагрузки
- Использование WMI

Техники распространения

- Использование удаленных сервисов
- Pass the Ticket / Pass the Hash
- Эксплуатация уязвимостей удаленных сервисов

Подходы к реализации

Самописное бинарное ВПО

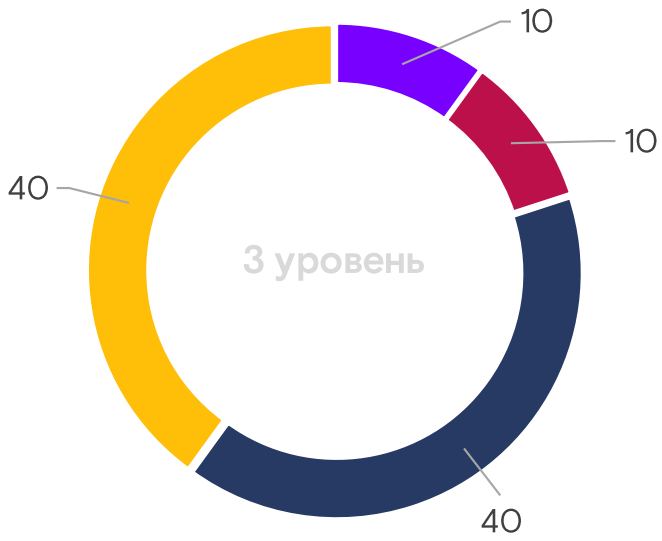
Использование легитимных утилит

Самописные скрипты

Инструменты для анализа защищенности, доступное ВПО

Ростелеком
Солар

Подходы к реализации



■ Самописное ВПО ■ Самописные скрипты ■ Легитимные утилиты ■ Доступное ВПО и фреймворки

Ключевые выводы

Существенный рост числа атак на субъекты КИИ

Рост числа потенциально опасных утилит в открытом доступе

Необходимость в сложных системах защиты

Вопросы спикеру

Артем Кильдюшев

Руководитель группы пресейла Solar JSOC
компании «Ростелеком-Солар»

Контакты

+7 (499) 755-07-70

presale@rt-solar.ru

Ростелеком
Солар