Ростелеком
Солар

«Ростелеком-Солар»

2020

«Ростелеком-Солар» защищает клиентов еще надежнее благодаря отчетам «Лаборатории Касперского» об APT-угрозах

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky
Threat Intelligence

«Ростелеком-Солар»

https://rt-solar.ru/about_company/

Solar JSOC — первый коммерческий SOC в РФ

- Более 200 экспертов по безопасности
- Более 110 клиентов из числа крупных российских компаний
- Более 10 лет опыта реализации ИБ-проектов национального масштаба
- Крупнейший центр защиты от киберугроз и провайдер сервисов ИБ в России
- Сотрудничает с ФинЦЕРТ Банка России и НКЦКИ ФСБ России

Компания «Ростелеком-Солар» предоставляет сервисы и технологии для целевого мониторинга, оперативного управления информационной безопасностью (ИБ) и защиты информационных активов. Solar Security (прежнее название компании) была одной из первых российских организаций, занимающихся целевым мониторингом и управлением ИБ, а в 2018 году вошла в состав группы компаний «Ростелеком». Центр мониторинга и реагирования Solar JSOC на данный момент является крупнейшим в России.

У «Ростелеком-Солар» есть филиалы в Москве, Нижнем Новгороде, Самаре и Хабаровске, что позволяет осуществлять мониторинг угроз 24 часа в сутки без перерывов и выходных. Среди клиентов Solar JSOC – крупные российские организации и госструктуры, такие как Росфинмониторинг, НСПК, Leroy Merlin, Тинькофф, УБРиР и др.

«Мы стремимся предоставить клиенту максимальную защиту: круглосуточно отслеживаем состояние систем и оперативно реагируем на инциденты. Ни одна атака не должна остаться незамеченной. Поэтому мы постоянно расширяем и совершенствуем наши знания о тактике и инструментарии киберпреступников».

Тимур Ниязов,
руководитель направления мониторинга и реагирования на киберугрозы «Ростелеком-Солар»

Проблематика

Компания «Ростелеком-Солар» предоставляет такие услуги, как:

- мониторинг, реагирование и анализ инцидентов;
- контроль защищенности и управление уязвимостями;
- анализ безопасности состояния конфигураций систем ИБ;
- техническое расследование инцидентов.

Чтобы обеспечить своим клиентам эффективную защиту, специалисты компании должны быть в курсе тактик и методов, которыми пользуются киберпреступники. Чем более полным представлением о потенциальных угрозах владеют эксперты, тем проще выработать грамотную стратегию защиты и тем больше шансов, что инцидент удастся предотвратить или локализовать на ранней стадии.

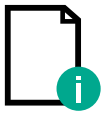
Поскольку «Ростелеком-Солар» работает с крупными организациями, в том числе государственными, компании важно иметь доступ к максимально подробной информации о действующих APT-группировках и их инструментарии. Поэтому помимо материалов собственных расследований организация привлекает к работе дополнительные данные. В открытых источниках публикуется далеко не вся информация об APT-атаках, и руководство «Ростелеком-Солар» было заинтересовано в партнерстве с компанией, отслеживающей большое количество APT-группировок, в том числе действующих на территории России.

Решение

Компания «Ростелеком-Солар» остановила свой выбор на аналитических отчетах «Лаборатории Касперского» об APT-угрозах. В отчеты входит подробное описание вредоносных кампаний, в том числе отрасли и регионы, которых они коснулись, и вероятные цели злоумышленников. Также подписчикам предоставляют детальный технический анализ атак и инструментария киберпреступников, список индикаторов компрометации (IoC) и YARA-правил, которые можно в дальнейшем применять для защиты клиентов.

Эксперты «Лаборатории Касперского» следят за деятельностью более 100 APT-группировок в 85 странах мира. Благодаря широкому охвату отчеты предоставляют исчерпывающую картину актуального ландшафта угроз.

«Отчеты об APT-угрозах помогают своевременно отразить наиболее разрушительные кибератаки. Учитывая, что подобные атаки нередко угрожают критическим активам, наше сотрудничество «Ростелеком-Солар» имеет важное стратегическое значение. «Ростелеком-Солар» является одним из ведущих игроков на рынке управления информационной безопасностью, и клиенты компании могут быть уверены, что все решения, принимаемые специалистами центра Solar JSOC, основаны на самой достоверной и актуальной информации», — говорит Сергей Земков, Управляющий директор, Россия и страны СНГ.



Актуальные сведения о наиболее опасных угрозах

Эксперты команды GReAT «Лаборатории Касперского» следят за деятельностью более 100 группировок, выявляют сложные и опасные целевые атаки и новейшие тенденции в сфере киберпреступности в 85 странах.

Доступ к результатам конфиденциальных расследований

Большинство расследований не публикуется из соображений конфиденциальности. Клиенты «Лаборатории Касперского» получают доступ к закрытым отчетам о киберинцидентах.

Актуальные сведения для технических специалистов и директоров ИБ

Отчеты «Лаборатории Касперского» содержат подробную информацию о вредоносных кампаниях, в том числе список индикаторов компрометации (IoC) и YARA-правил.

«Для нашего центра мониторинга, обслуживающего более сотни крупных организаций, постоянный сбор и обновление информации об угрозах – одна из ключевых задач, поэтому мы стремимся сотрудничать с ведущими поставщиками информации об актуальных угрозах. Такой подход помогает нам оперативно выявлять и уже на входе отражать кибератаки на наших клиентов, а значит, сохранять лидерство в сфере предоставления сервисов информационной безопасности».

Тимур Ниязов,
руководитель направления мониторинга и реагирования на киберугрозы «Ростелеком-Солар»

Результаты

Компания «Ростелеком-Солар» оформила трехлетнюю подписку на аналитические отчеты «Лаборатории Касперского». Сведения, предоставленные партнером, вместе с данными собственных расследований позволили специалистам «Ростелеком-Солар» составить четкое представление об актуальных угрозах и выстроить эффективную стратегию защиты клиентов.

Индикаторы компрометации и YARA-правила «Лаборатории Касперского» дополнили собственную базу поставщика услуг по информационной безопасности. С помощью этих сведений эксперты «Ростелеком-Солар» могут обнаруживать целевые атаки на ранних стадиях и принимать меры по реагированию на инцидент, пока ущерб от действий злоумышленников не достиг разрушительных масштабов.