



## PT MULTISCANNER: ЗАЩИТА ОНЛАЙН-СЕРВИСА ПРИЕМА ДОКУМЕНТОВ

«В условиях, когда страхователи самостоятельно могут загружать документы на онлайн-сервис, риск того, что в нашу систему попадет зараженный файл, многократно вырос. Поэтому одна из задач, стоящих перед нами, — обеспечить оперативное обнаружение и своевременное блокирование вирусов. Для этого была выбрана система выявления вредоносного контента PT MultiScanner компании Positive Technologies. Интеграция системы с нашим онлайн-сервисом и другими системами защиты позволила повысить безопасность наших корпоративных ресурсов».

**Андрей Поломошнов,**  
заведующий сектором эксплуатации  
средств защиты информации  
СПАО «Ингосстрах»



### ПРОФИЛЬ ОРГАНИЗАЦИИ

- + **Название:** «Ингосстрах»
- + **Отрасль:** страхование
- + **География:** Россия, Белоруссия, Армения, Киргизия, Узбекистан, Казахстан, Азербайджан, Китай, Индия
- + **Объем премий за 2016 год:** 92,3 млрд руб.
- + **Договоры ОСАГО:** более 2 млн

- + **Решение:** PT MultiScanner для комплексной антивирусной проверки файлов, загружаемых через личный веб-кабинет или терминалы в офисах

### ЗАДАЧА

Всеобщая цифровая трансформация оказывает сильное влияние на страховой бизнес. Страховые компании, вне зависимости от специализации, предлагают своим клиентам возможность отправлять заявления и предоставлять необходимые документы в страховую компанию не выходя из дома — по электронной почте, через официальные сайты и онлайн-сервисы дистанционного урегулирования убытков.

Однако эти нововведения открывают широкие возможности злоумышленникам и делают уязвимой для вторжений ИТ-инфраструктуру страховых компаний. Атаки на веб-сервисы с последующим заражением инфраструктуры вредоносным программным обеспечением — по-прежнему самый распространенный тип атак. В связи с выходом нового онлайн-сервиса приема документов по страховым случаям (КАСКО и ОСАГО) крупнейшей российской страховой компании «Ингосстрах» требовалось решение, которое бы обеспечило:

- + высокий уровень детектирования вредоносного ПО,
- + защиту в реальном времени,
- + учет особенностей функционирования онлайн-сервиса,
- + совместимость с существующей инфраструктурой и бизнес-процессами,
- + возможность масштабирования и работу под нагрузкой.

### РЕШЕНИЕ

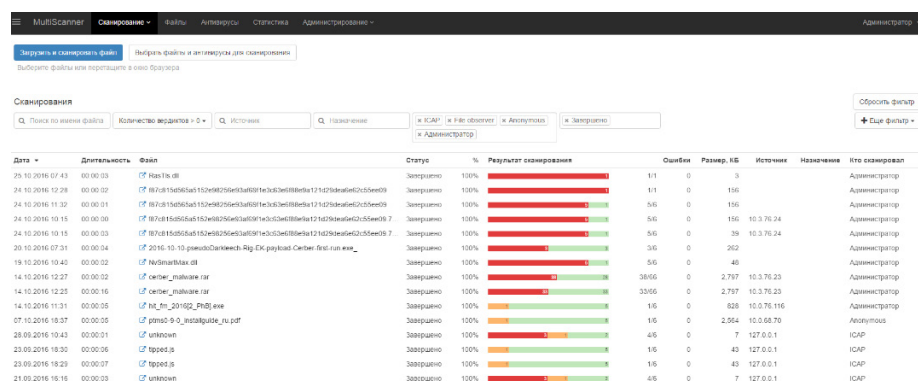
Для решения поставленной задачи была выбрана система выявления вредоносного контента PT MultiScanner компании Positive Technologies. Эксперты компании проанализировали работу онлайн-сервиса приема документов и сформировали рекомендации по обеспечению комплексной безопасности. В соответствии с ними эксперты «Ингосстраха» при поддержке специалистов Positive Technologies реализовали поддержку протокола ICAP, установили и настроили ICAP-клиент. Далее специалисты вендора адаптировали и настроили PT MultiScanner с учетом архитектуры онлайн-сервиса и ИТ-инфраструктуры страховой компании. В итоге система PT MultiScanner была успешно интегрирована в существующую инфраструктуру.

## КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- + Многоядерная проверка объектов на вирусы
- + Офлайн-обновление баз
- + Безопасная работа с сервисами репутаций
- + Масштабирование
- + Ретроспективный анализ
- + Широкие возможности для интеграции (SIEM, WAF и др.)

«Тесное взаимодействие со специалистами "Ингосстраха" позволило оперативно доработать продукт с учетом технических особенностей сервиса и интегрировать PT MultiScanner в существующую инфраструктуру заказчика. Для нас этот проект является бесценным опытом совместного проектирования механизмов безопасности веб-сервиса, начиная с ранних этапов его разработки», — комментирует внедрение Евгения Красавина, руководитель отдела продвижения и развития продуктов Positive Technologies.

Существующая в компании система противодействия угрозам была усилена рядом уникальных возможностей PT MultiScanner — потоковым сканированием на нескольких антивирусных ядрах, ретроспективным анализом объектов, конфиденциальным использованием репутационных сервисов. Благодаря широким интеграционным возможностям созданная система защиты в будущем сможет легко адаптироваться к росту нагрузки или изменениям в отраслевых требованиях по безопасности.



Дата	Длительность	Файл	Статус	%	Результат сканирования	Опции	Размер, КБ	Источники	Назначение	Кто сканировал
25.10.2016 07:43	00:00:03	Ⓜ Kacta.db	Завершено	100%		111	0	3		Администратор
24.10.2016 12:29	00:00:03	Ⓜ 882624480a6115c4e925e63a8091e3c34e185a1e1214210e4a1c2c5e0d9.7	Завершено	100%		5,6	0	166		Администратор
24.10.2016 11:32	00:00:01	Ⓜ 882624480a6115c4e925e63a8091e3c34e185a1e1214210e4a1c2c5e0d9.7	Завершено	100%		5,6	0	166		Администратор
24.10.2016 10:15	00:00:00	Ⓜ 882624480a6115c4e925e63a8091e3c34e185a1e1214210e4a1c2c5e0d9.7	Завершено	100%		5,6	0	166	10.3.76.24	Администратор
24.10.2016 07:31	00:00:03	Ⓜ 2016.10.10.pskovos.pskovos.Rip.CK.pskovos.Serby.fst.ran.eee_	Завершено	100%		5,6	0	39	10.3.76.24	Администратор
20.10.2016 07:31	00:00:04	Ⓜ 2016.10.10.pskovos.pskovos.Rip.CK.pskovos.Serby.fst.ran.eee_	Завершено	100%		5,6	0	252		Администратор
19.10.2016 10:42	00:00:02	Ⓜ NvSmbMax.db	Завершено	100%		5,6	0	48		Администратор
14.10.2016 12:27	00:00:02	Ⓜ seker_makave.rar	Завершено	100%		38,056	0	2,737	10.3.76.23	Администратор
14.10.2016 12:23	00:00:16	Ⓜ seker_makave.rar	Завершено	100%		33,056	0	2,737	10.3.76.23	Администратор
14.10.2016 11:31	00:00:05	Ⓜ ht_fm_201602_P8B.exe	Завершено	100%		1,6	0	828	10.0.76.116	Администратор
07.10.2016 18:37	00:00:05	Ⓜ ptmso-9_0_instalguide_ru.pdf	Завершено	100%		1,6	0	2,854	10.0.68.70	AccessPoint
28.09.2016 10:42	00:00:01	Ⓜ mltosn	Завершено	100%		4,8	0	7	127.0.0.1	ICAP
23.09.2016 18:30	00:00:06	Ⓜ tprosls	Завершено	100%		1,6	0	43	127.0.0.1	ICAP
23.09.2016 18:23	00:00:07	Ⓜ tprosls	Завершено	100%		1,6	0	43	127.0.0.1	ICAP
21.09.2016 16:16	00:00:03	Ⓜ mltosn	Завершено	100%		4,8	0	7	127.0.0.1	ICAP

## РЕЗУЛЬТАТ

Совместная работа PT MultiScanner с другими защитными системами позволяет компании «Ингосстрах» контролировать поступающий извне контент, противодействовать угрозам, выявлять распределенные во времени атаки и расследовать инциденты. Таким образом обеспечивается безопасная загрузка файлов через терминалы в офисах компании, а также через личный кабинет пользователя на сайте [www.ingos.ru](http://www.ingos.ru).

## О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.