

Решения Positive Technologies для коммерческих предприятий

Логинов Роман
Менеджер по продвижению продуктов

POSITIVE TECHNOLOGIES

ptsecurity.com

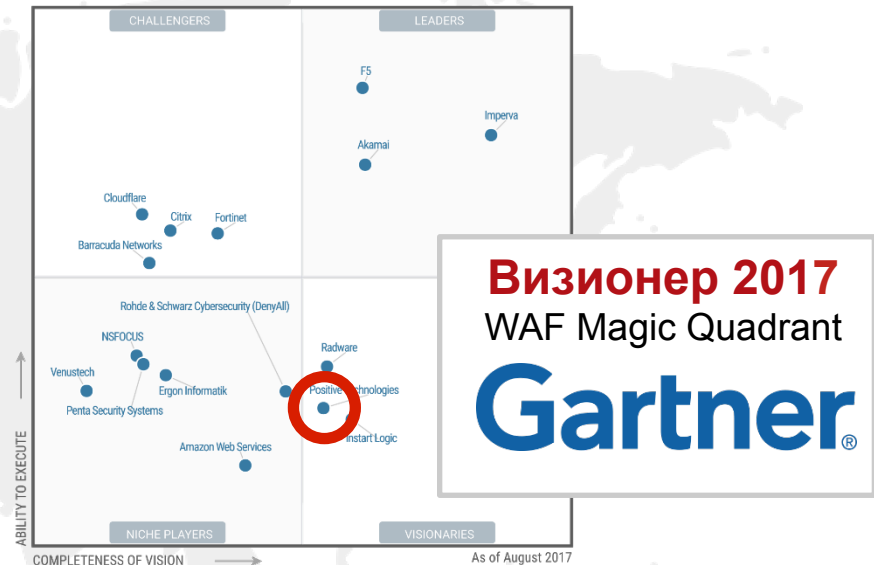
200+

аудитов безопасности
корпоративных систем

200+

обнаруженных
уязвимостей
нулевого дня

Главные продукты



16

лет исследований
и экспертизы

150+

уязвимостей нулевого дня
в системах SCADA

50+

расследований взломов
инфраструктуры

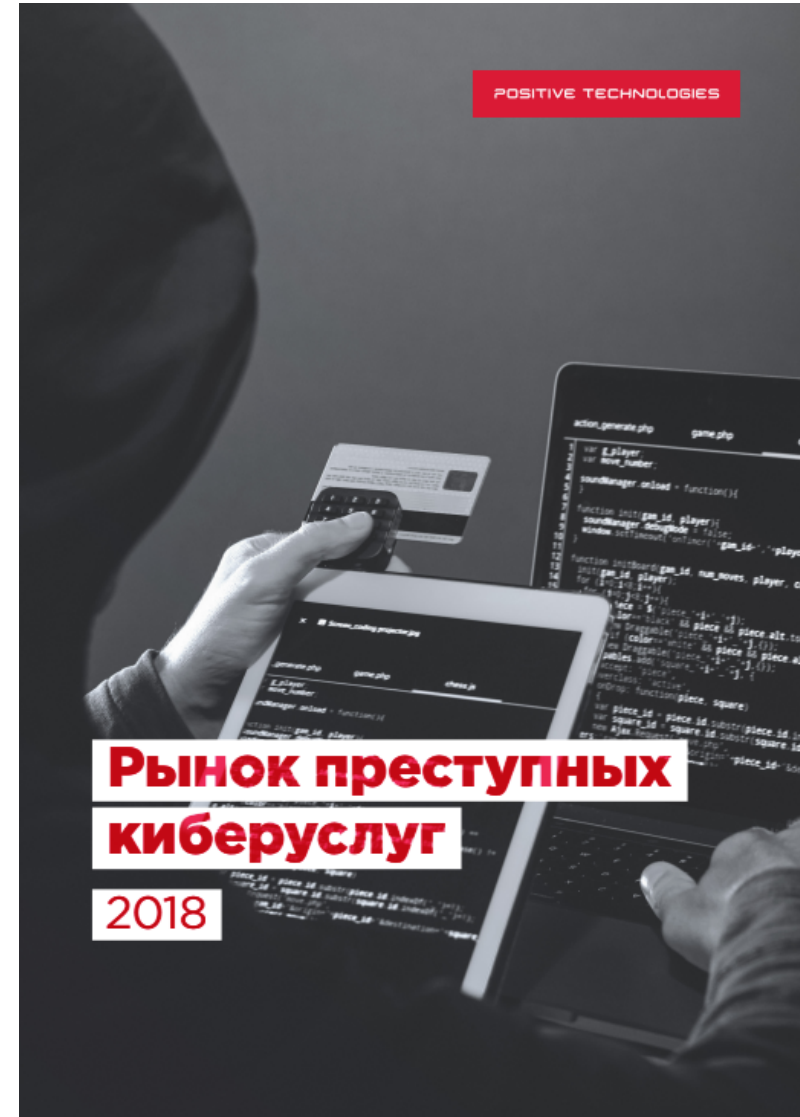
500+

исследований безопасности
мобильных и веб-приложений



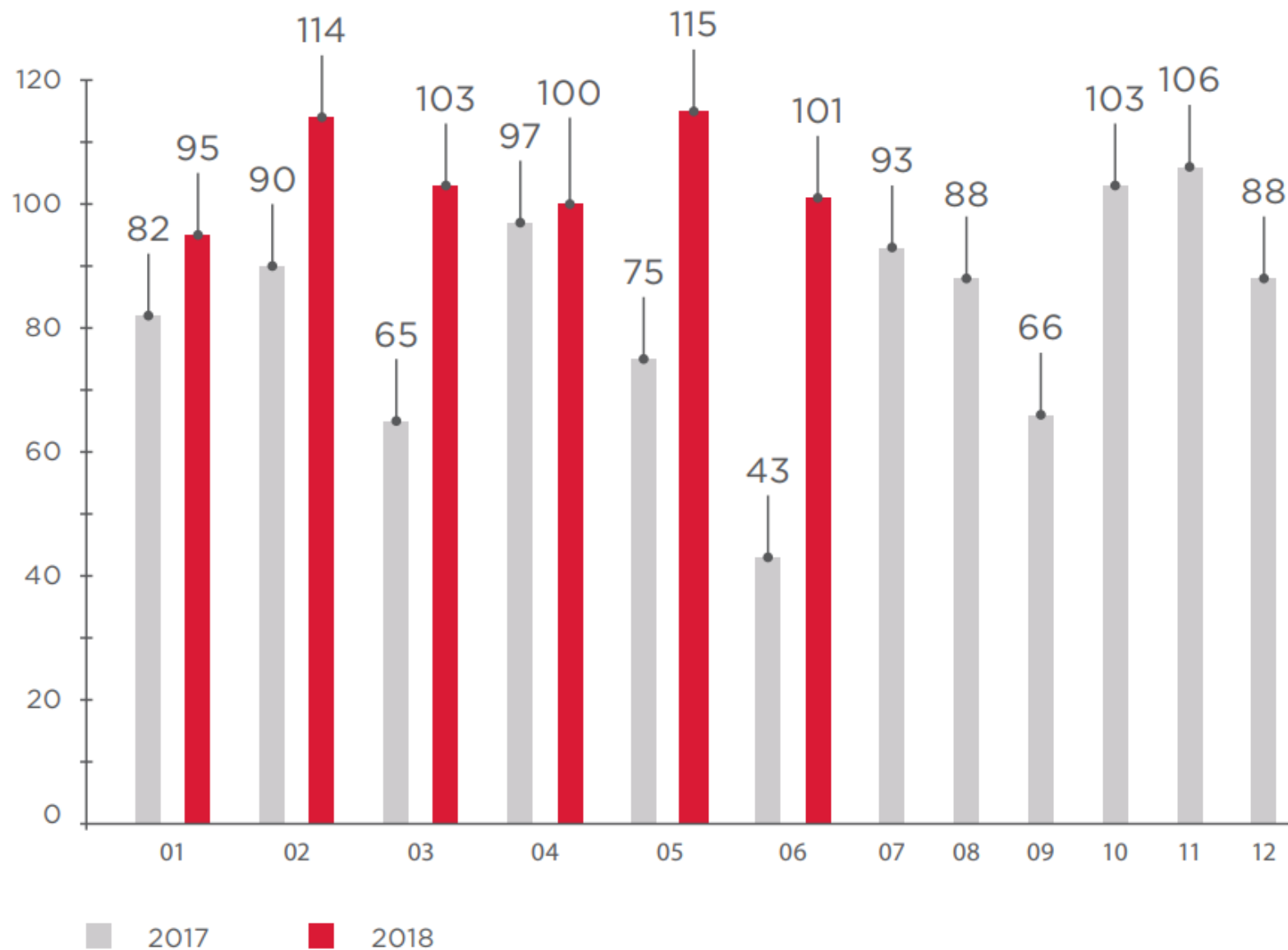
**Актуальные
киберугрозы**

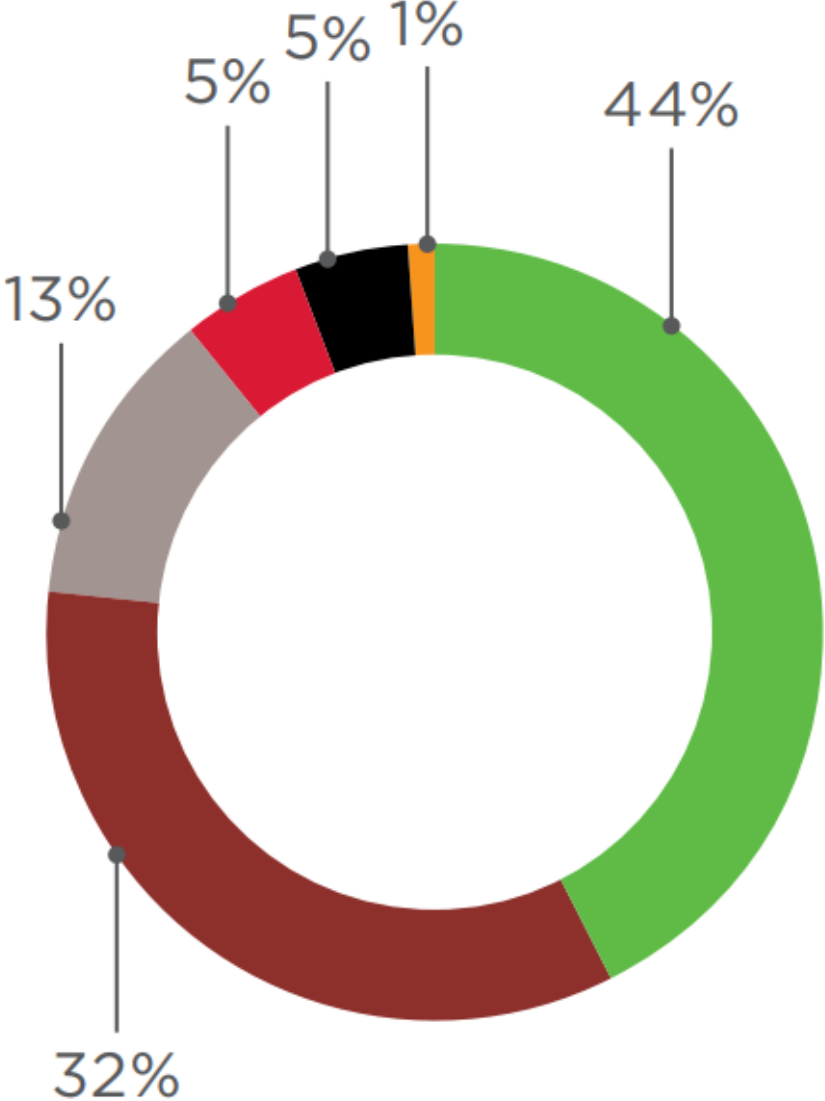
II квартал 2018 года



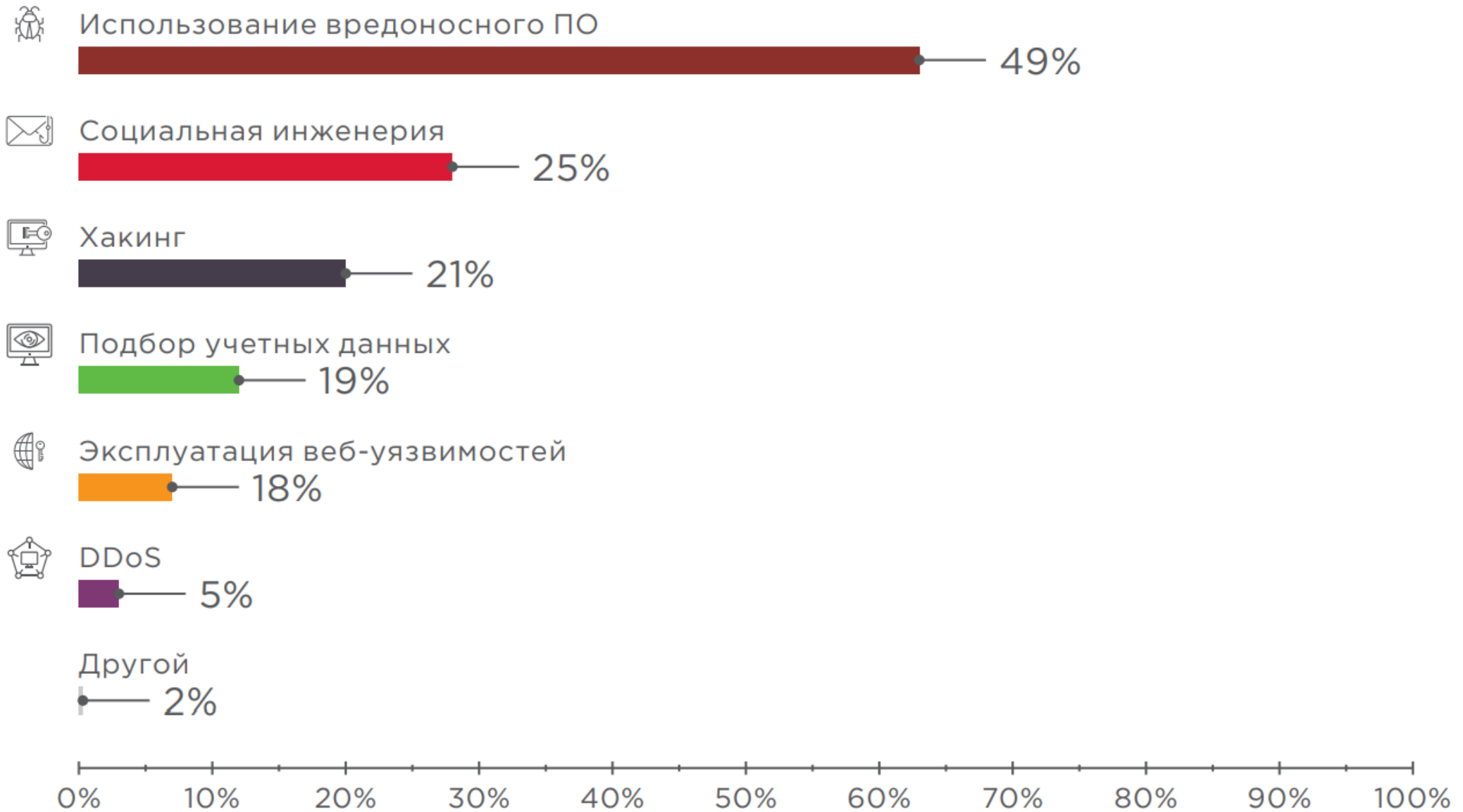
**Рынок преступных
киберуслуг**

2018





- Инфраструктура
- Веб-ресурсы
- Пользователи
- Мобильные устройства
- IoT
- Банкоматы и POS-терминалы

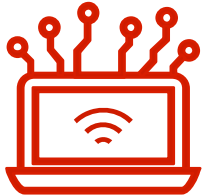


MaxPatrol 8

Контроль защищенности
и соответствия стандартам



**Слабые
пароли**



**Небезопасные
беспроводные сети**



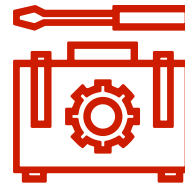
**Уязвимости
веб-приложений**



**Программное
обеспечение**



**Социальная
инженерия**



Ошибки в настройках:

- сетевого оборудования
- систем защиты периметра
- веб-приложений
- баз данных



- Требуется наличие узкопрофильных специалистов
- Длительное время обслуживания каждого компонента ИС
- Высокая роль человеческого фактора



- + Использует единые подходы для анализа всех компонентов ИС
- + Производится на регулярной основе автоматически
- + Формирует унифицированную отчетность



The screenshot displays the Positive Technologies Audit application interface. The left pane, titled "Навигатор", shows a tree view of system components. The right pane, titled "Информация", displays details for a selected vulnerability.

Навигатор

- Сортировка ▾ Узел ▾ Журнал
- 192.168.53.20
 - Microsoft .NET Framework
 - Microsoft Internet Explorer
 - Microsoft JScript
 - Microsoft Pragmatic General Multicast
 - Microsoft VBScript
 - Microsoft Windows
 - Microsoft Windows Media
 - Удаленное выполнение кода в Windows Media Player, связанное с DataObject
 - Удаленное выполнение кода, связанное с видеodeкодером WMV
 - Удаленное выполнение кода, связанное с обработкой мультимедиа
 - Удаленное выполнение кода, связанное с обработкой мультимедиа
 - Microsoft XML Core Services
 - 3.0
 - 6.0
 - Уязвимость в MSXML XSLT
 - Разглашение информации, связанное с MSXML
 - Уязвимость, связанная с URI сущности MSXML
 - Quartz.dll (DirectShow)
 - Remote Desktop Connection Client
 - Небезопасная загрузка библиотек в Remote Desktop
 - Повышение привилегий, связанное с обходом каталога
 - Удаленное выполнение кода, связанное с элементом управления ActiveX удаленных рабочих столов
 - Подмена данных узла сеансов удаленных рабочих столов
 - Windows Media Center
 - Windows Defender
 - Hardware Information
 - Информация о BIOS
 - Информация о CPU
 - Информация о жестких дисках
 - Информация о материнской плате
 - Информация о памяти
 - Информация о сетевых картах
 - Network Configuration
 - MAC-адрес сканируемого адаптера
 - Доступные сетевые подключения
 - Открытые порты по прослушиваемым адресам
 - Список открытых портов
 - Operating System
 - Список процессов

Информация

Серьезная уязвимость
Удаленное выполнение кода в Windows Media Player, связанное с DataObject
ID: 413741
CVE: CVE-2015-1728
fstec: BDU:2015-12135
Дата публикации: 09.06.2015

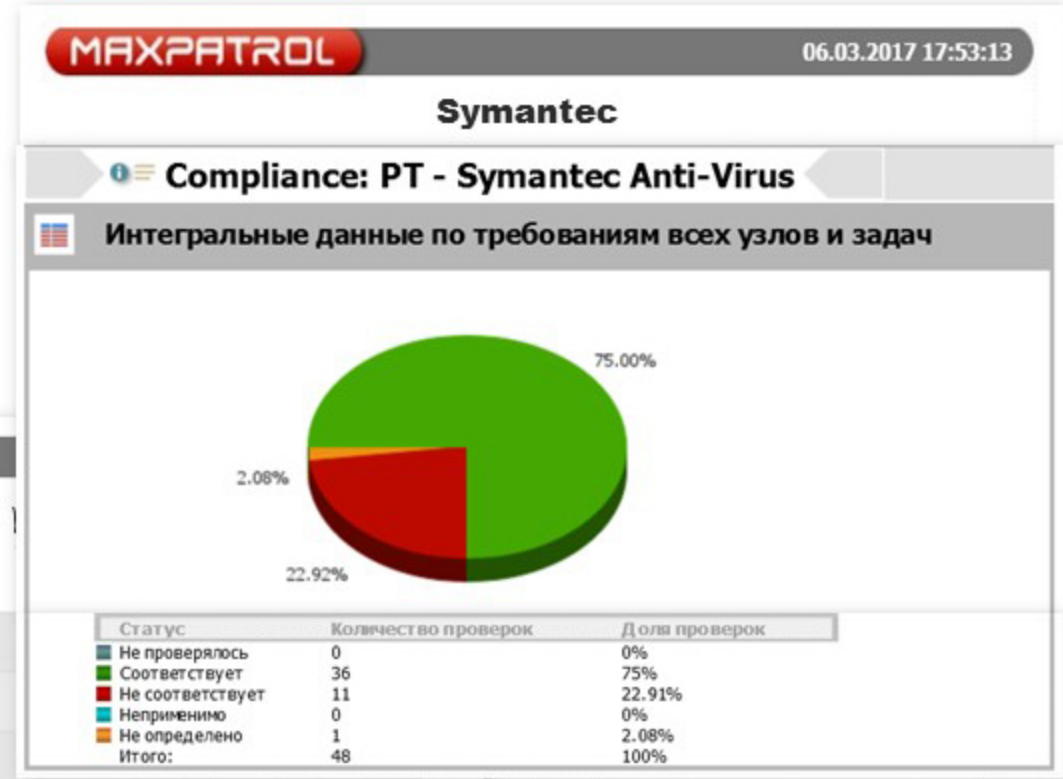
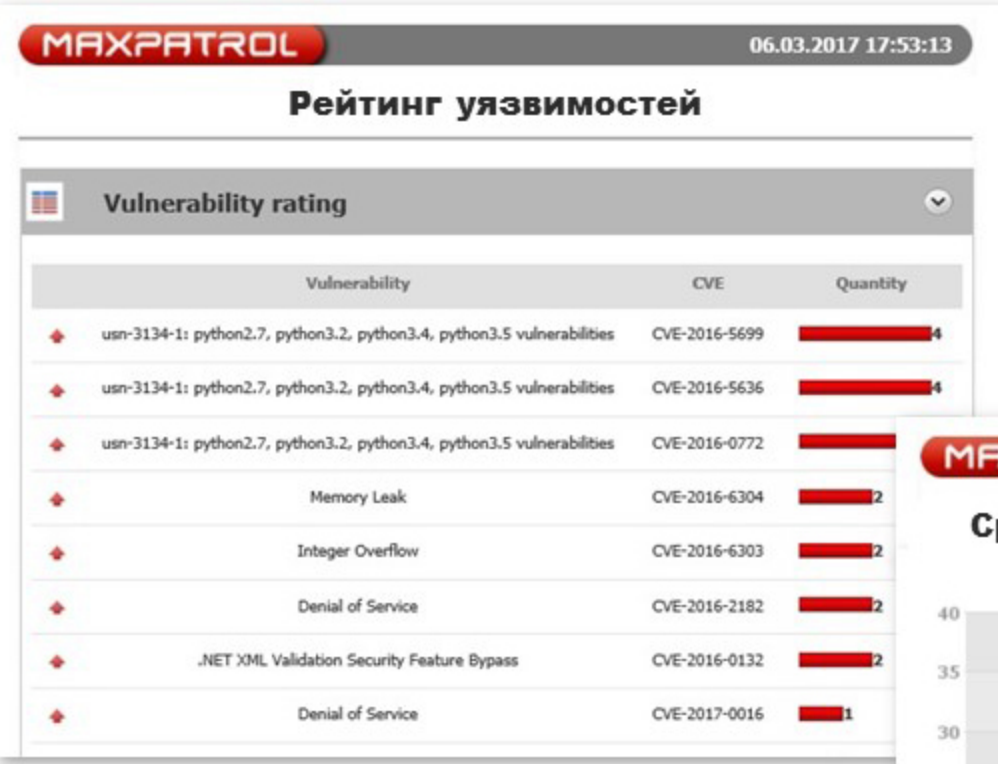
Краткое описание
Уязвимость позволяет злоумышленнику получить полный контроль над системой.

Описание
Уязвимость, позволяющая удаленно выполнить код, существует в Windows Media Player и связана с обработкой специально сформированных DataObjects. Эксплуатация данной уязвимости позволяет злоумышленнику, действующему удаленно, получить полный контроль над системой; после чего он может устанавливать программы, просматривать, изменять или удалять данные, а также создавать новые учетные записи с полными правами пользователя. Пользователи, права которых в системе ограничены, менее подвержены данной уязвимости, чем пользователи, работающие с правами администратора. Для эксплуатации данной уязвимости пользователь должен открыть специально сформированный DataObject в Windows Media Player.

Как исправить
Используйте рекомендации производителя:
<http://technet.microsoft.com/security/bulletin/ms15-057>

Ссылки
MS (15-057): <http://technet.microsoft.com/security/bulletin/ms15-057>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1728>

CVSS
Базовая оценка: 9.3 (AV:N/AC:M/Au:N/C:C/I:A/C)
Временная оценка: 6.9 (AV:N/AC:M/Au:N/C:C/I:A/C/E:U/RL:OF/RC:C)
AV:N данная уязвимость может эксплуатироваться удаленно
AC:M для эксплуатации уязвимости нужна дополнительная информация или нестандартная конфигурация уязвимого ПО
Au:N для эксплуатации уязвимости проходить аутентификацию не требуется



MaxPatrol SIEM

Выявление инцидентов ИБ в реальном времени

Растет разрыв между моментом компрометации и обнаружением

POSITIVE TECHNOLOGIES

62%

результативных атак являются целевыми

3
года

в среднем злоумышленник присутствует в системе

10%

атак выявляются самими жертвами

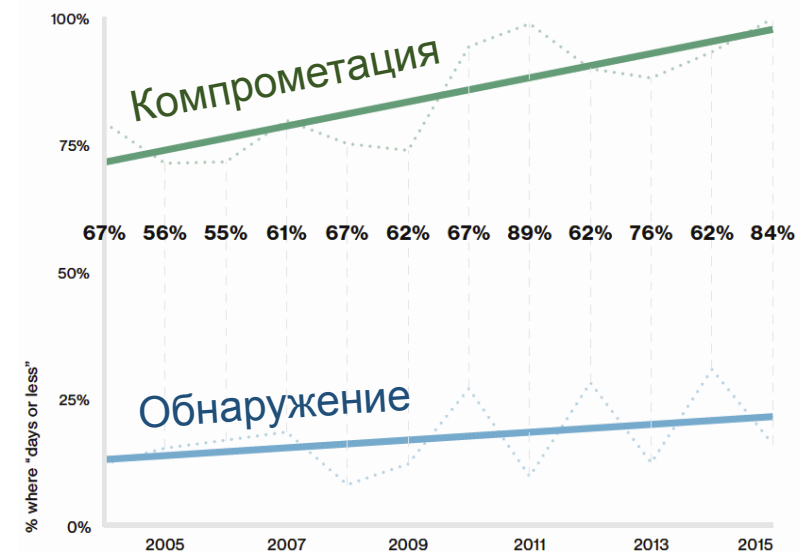
Источник: [Кибербезопасность 2016–2017: от итогов к прогнозам](#) (Positive Technologies)



Дни, часы, минуты
занимает компрометация



Недели, месяцы
проходят до обнаружения



MaxPatrol SIEM

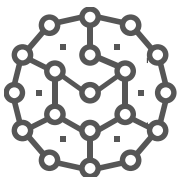
- Контролирует состояние IT-инфраструктуры в любой момент времени.
- Выявляет инциденты даже после изменений IT-ландшафта.
- Автоматически предоставляет ИБ-экспертизу в продукт, выявляет новые угрозы и помогает расследовать инциденты.





Контроль
IT-инфраструктуры

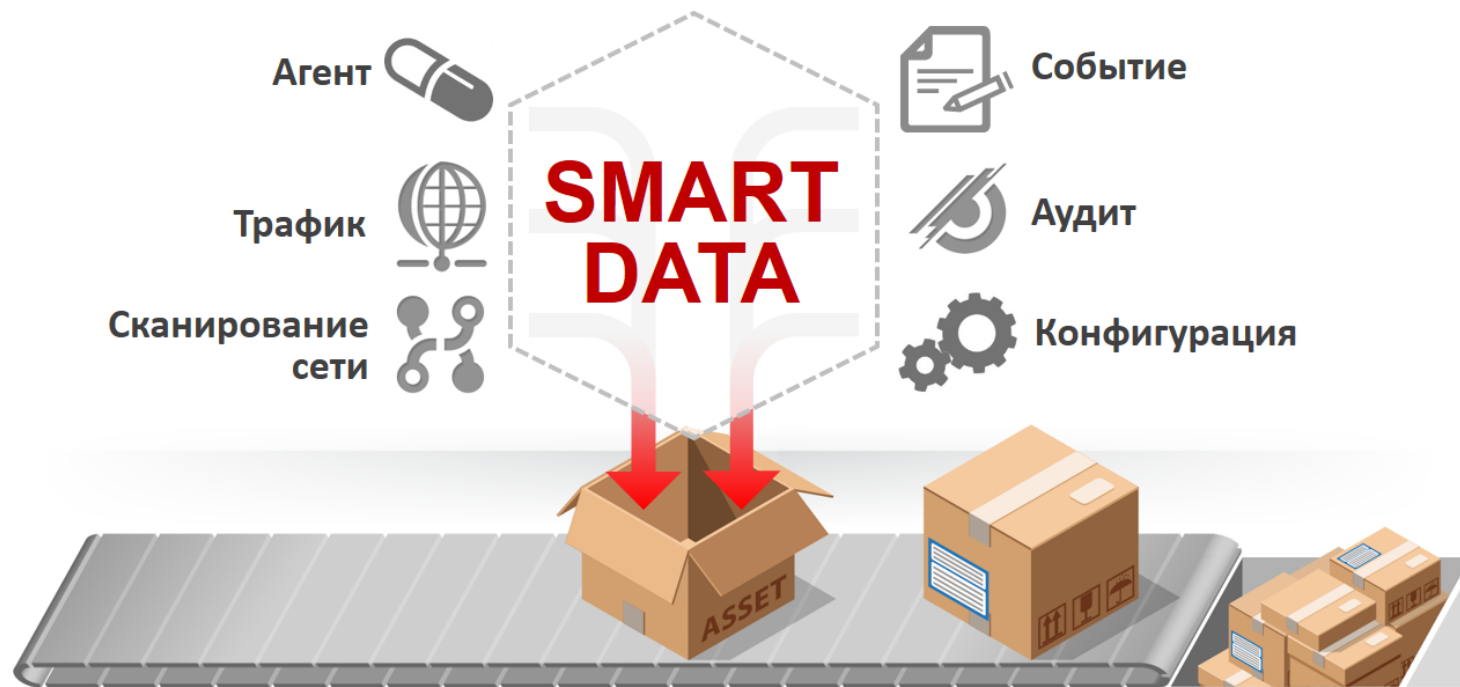
- Автоматически строит полную модель IT-инфраструктуры.
- Постоянно обогащается новыми данными об IT-активах.
- Автоматически идентифицирует IT-активы даже после изменения IP- и MAC-адреса и других характеристик.



Адаптация
к изменениям



Профилактика
угроз

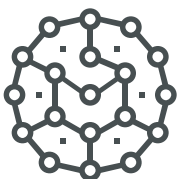


MaxPatrol SIEM: полная и точная модель IT-активов

POSITIVE TECHNOLOGIES



Контроль
IT-инфраструктуры



Адаптация
к изменениям



Профилактика
угроз

MaxPatrol SIEM:

- Упорядочивает данные об инфраструктуре в IT-активы и их взаимодействия
- Автоматически присваивает значимость IT-активам и приоритизирует на ее основе инциденты
- Собирает и хранит не логи, а состояния каждого IT-актива во времени

Паспорт IT-актива и история актива

10.0.208.165 (dc01-iis01.ptsecurity.com)

Обнаружен 27 окт 2015 → Последнее обновление 12 фев 2016 → Ус...

↑ 9968,8 | Средняя значимость

История за 23-24 апреля

Интегр. уязвимость

Сканирования

Ручной ввод

Сводка | Уязвимости | Конфигурация | Метрики CVSS

Информация о системе

OS	Windows 2012 6.3.9600
BIOS	Phoenix Technologies LTD PhoenixBIOS 4.0 Release 6.0
CPU	Intel(R) Xeon(R) CPU E5-2650 v2 @ 2.60GHz Intel(R) Xeon(R) CPU E5-2650 v2 @ 2.60GHz
MB	Intel Corporation
RAM	32
HDD	\\.\PHYSICALDRIVE0
Ethernet	vmxnet3 Ethernet Adapter
Workgroup	WORKGROUP

Самые опасные уязвимости

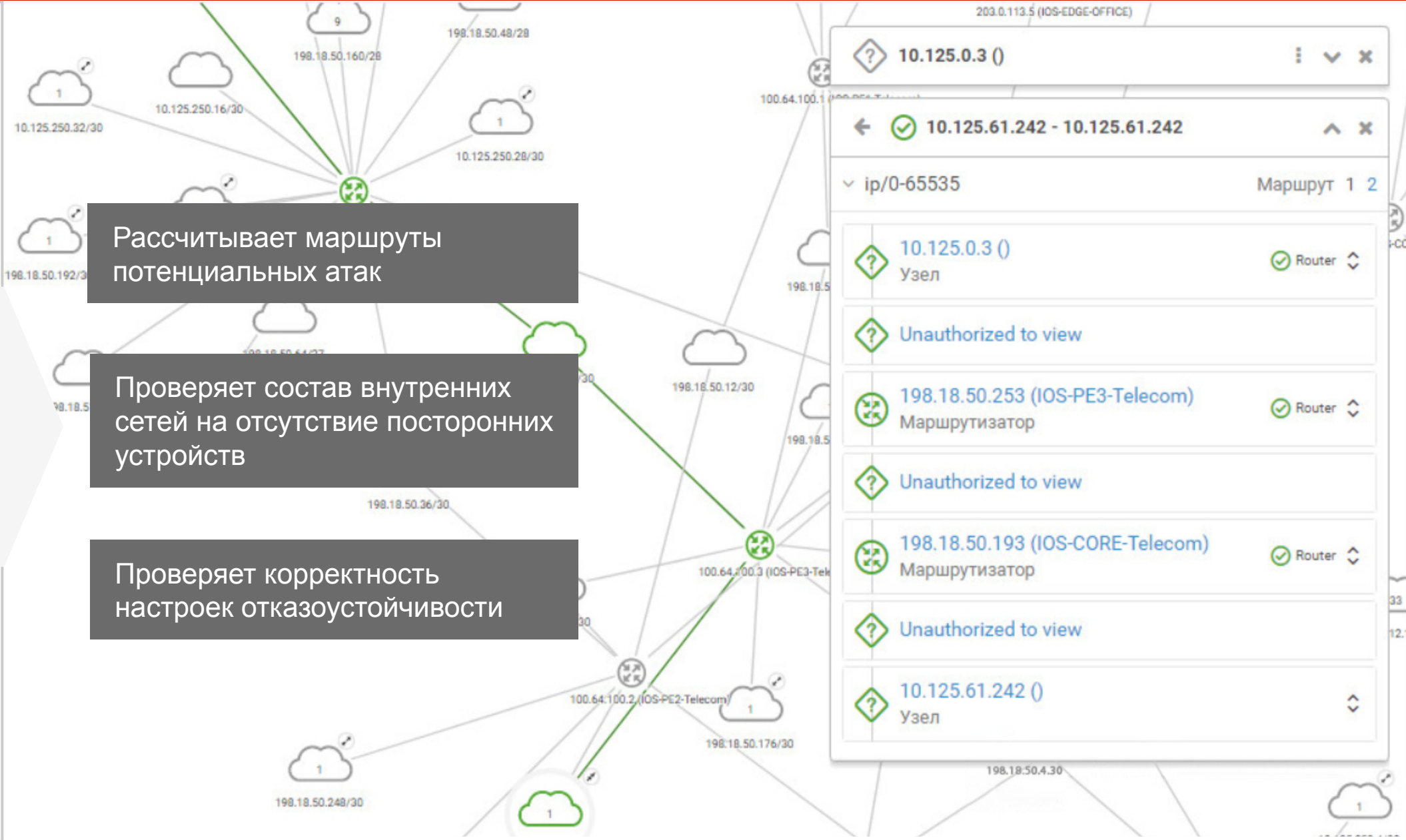
- ↑ Окончание поддержки продукта
- ↑ Окончание поддержки продукта
- ↑ Окончание поддержки продукта
- ↑ Окончание поддержки продукта
- ↑ Окончание поддержки продукта
- ↑ Окончание поддержки продукта
- ↑ Окончание поддержки продукта
- ↑ Отказ в обслуживании, связанный с TCP/IP версии 6 (IPv6)
- ↑ Повышение привилегий, связанное с обработкой шрифта TrueType
- ↑ Повышение привилегий, связанное с Win32k

Уязвимость сетевых служб

Network.Services.HttpSslService	6	■
Network.Services.SslService	6	■
Network.Services.RdpService	4	■
Network.Services.SmbOverNetbiosService	1	■

Сетевая конфигурация

Интерфейс	Порт	Сервис	ПО
> ip://[:1]			
> ip://[2001:db8:1329:0:1864:d733:12a8:7ccb]			
> ip://[2001:db8:cafe:1:1864:d733:12a8:7ccb]			



Рассчитывает маршруты
потенциальных атак

Проверяет состав внутренних
сетей на отсутствие посторонних
устройств

Проверяет корректность
настроек отказоустойчивости

MaxPatrol SIEM: модельные корреляции

POSITIVE TECHNOLOGIES



Классический
SIEM

MaxPatrol
SIEM



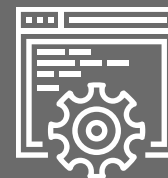
События

TCP Ports
Hardware Soft
Configs

Данные
актива



Корреляционные
правила



MaxPatrol SIEM автоматически адаптируется к изменениям IT-ландшафта.



Создает корреляции на основе данных IT-активов и динамических групп активов, а не логов.



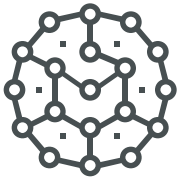
Правила корреляции продолжают выявлять угрозы после появления нового оборудования или изменения конфигурации сетевых узлов.

MaxPatrol SIEM: в каждом пакете обновлений РТ КВ

POSITIVE TECHNOLOGIES



Контроль
IT-инфраструктуры



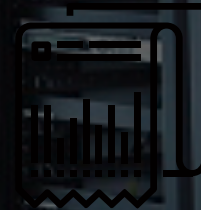
Адаптация
к изменениям



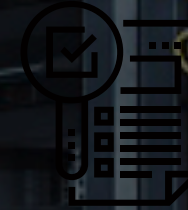
Профилактика
угроз



Новые правила
корреляции, агрегации,
нормализации



Информация о методах
и тактиках проведения атак,
индикаторы компрометации

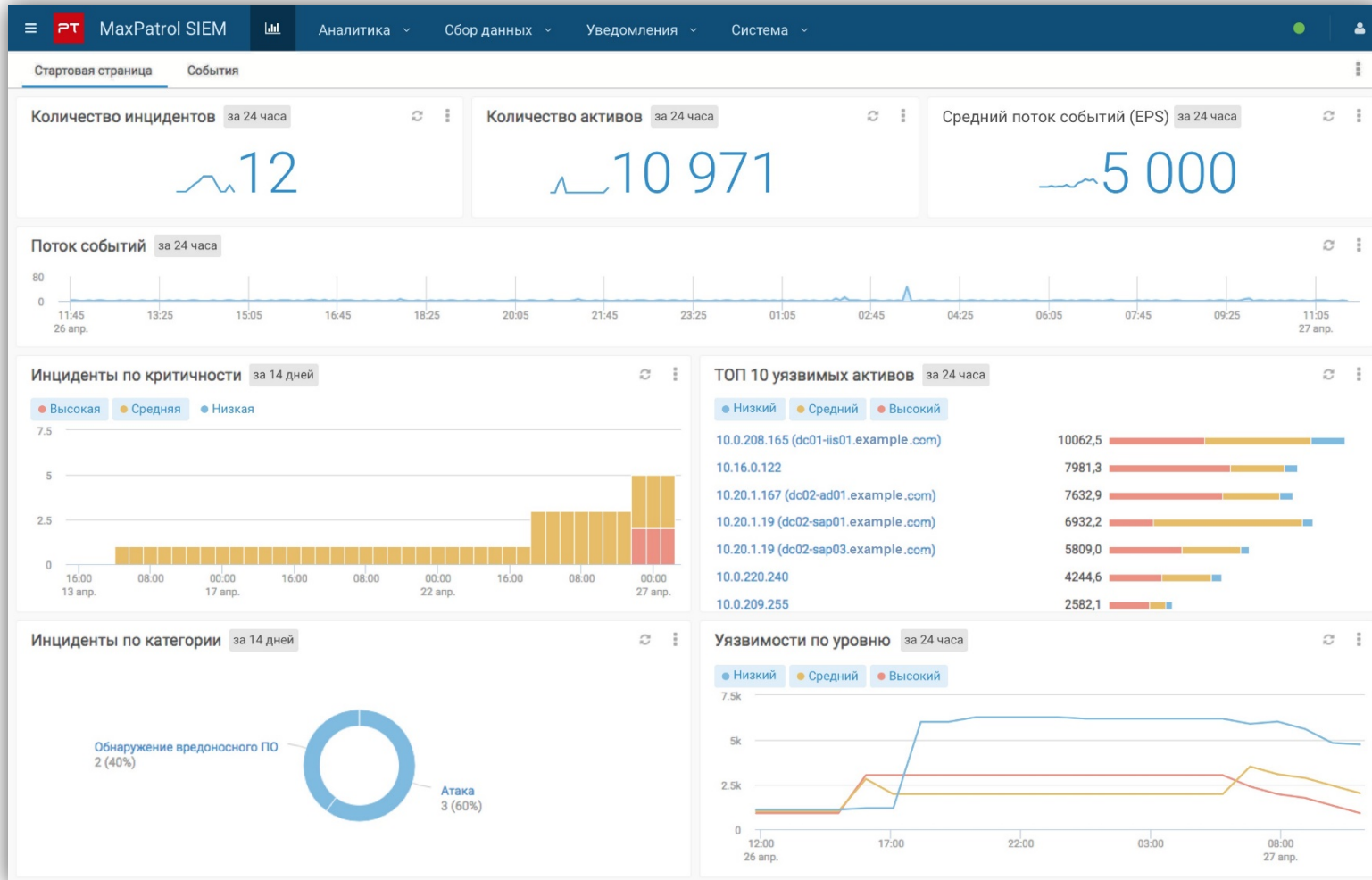


Рекомендации по сбору
информации из MP SIEM
для подтверждения инцидента
и его расследования



Рекомендации по тонкой
настройке аудита на источниках
для точного выявления атак





Настраиваемые дашборды и пользовательские виджеты

Детализация информации с дашбордов в один клик

Автоматическое создание отчетов

Отправка отчетов по расписанию

PT Application Firewall

Межсетевой экран уровня приложений

~3,5 млрд
активных
пользователей
(население ~7,3)*



Охватывает
практически все
сферы нашей жизни

Веб-приложения стали целью злоумышленников № 1

30%

30% атак приходится на веб-приложения*

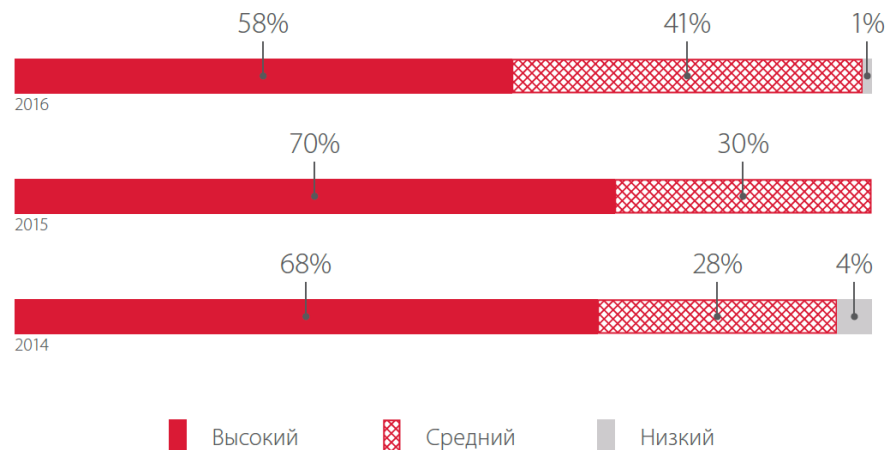
58%

58% веб-приложений содержат критически опасные уязвимости

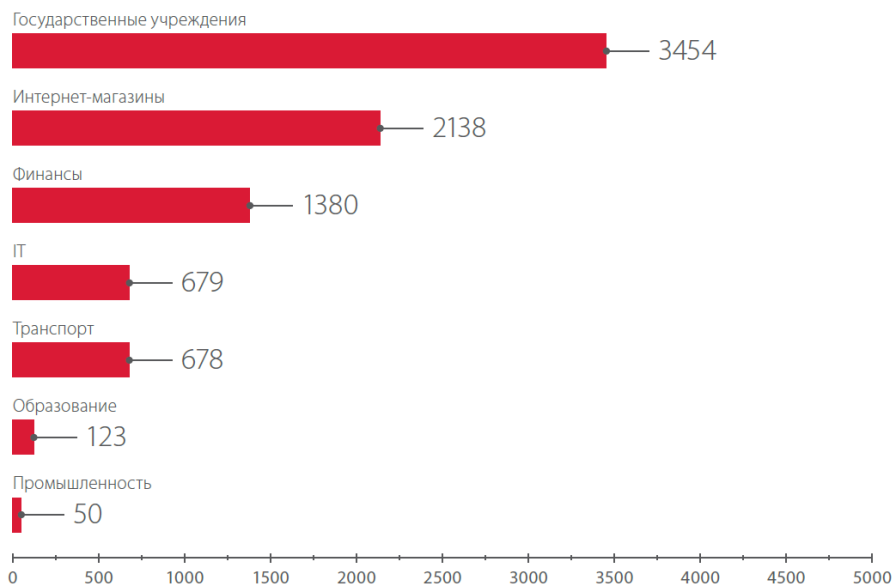
77%

В 77% случаев за периметр организации можно проникнуть через веб-уязвимости**

Также необходимо выполнять требования регуляторов (ФСТЭК, Банка России)

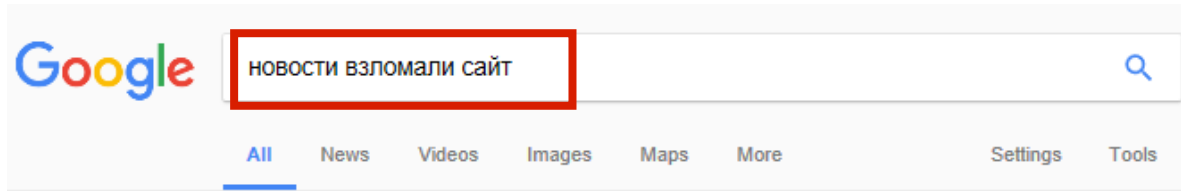


Доля уязвимых сайтов по степени риска уязвимостей



Среднее количество атак в день на одну систему

Источники:
* Verizon Data Breach report 2017
** Positive Research 2017



Page 3 of about 4,480,000 results (0.28 seconds)

[Хакеры ИГ взломали сайт губернатора Огайо — Sputnik / Новости](https://news.sputnik.ru/.../40812411a88a46ea0043d5cd5fbc56a7b...)
<https://news.sputnik.ru/.../40812411a88a46ea0043d5cd5fbc56a7b...> Translate this page
Сайты правительства американского штата Огайо подверглись хакерской атаке. На них появились сообщения в поддержку запрещенной в России ...

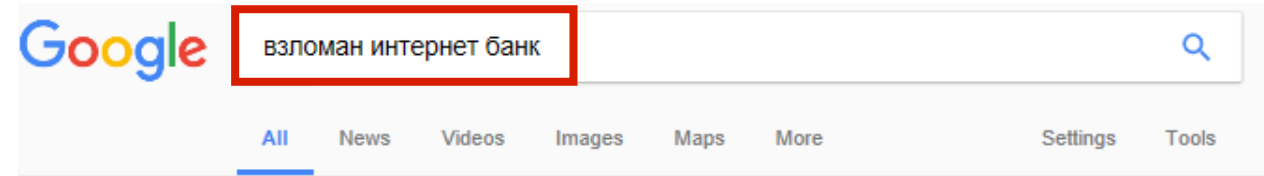
[Хакеры взломали сайт сахалинского ЗАГСа :: Технологии ...](https://sakhalinpacificplaza.ru/news/43435/)
<https://sakhalinpacificplaza.ru/news/43435/> - Translate this page
информационное агентство, citysakh, последние новости, новости ... В первом послании сообщается, что сайт взломан, но злоумышленники не будут ...

[Хакеры взломали сайт «Народной трибуны» ЛНР | Новости](https://riafan.ru/881615-khakery-vzломali-sait-narodnoi-tribuny-lnr)
<https://riafan.ru/881615-khakery-vzломali-sait-narodnoi-tribuny-lnr> Translate this page
Jul 24, 2017 - Луганск, 24 июля. Неизвестные хакеры осуществили кибератаку на один из официальных сайтов Луганской народной республики.

[Палестинские хакеры взломали сайт МЕРЕЦа | ILand | Новости](https://iland.tv/news/.../Палестинские_хакеры_взломали_сайт_M...)
https://iland.tv/news/.../Палестинские_хакеры_взломали_сайт_M... Translate this page
Jul 23, 2017 - Официальный сайт леворадикальной партии МЕРЕЦ в конце недели был взломан пропалестинскими хакерами. Об этом со...

[Хакеры взломали правительственные сайты Венесуэлы](https://petrimazepa.com/news/venezuela-the-binary)
<https://petrimazepa.com/news/venezuela-the-binary>
20 hours ago - Хакеры взломали правительственные сайты Венесуэлы, именуя себя «The Binary Guardians», ...

[Ташкентские хакеры взломали сайт Агентства по вопросам ...](https://nuz.uz)
<https://nuz.uz> > События Translate this page
Новости Узбекистана → События → Ташкентские хакеры взломали сайт ... Для удобства претендентов на сайте Агентства для перехода на сайт ...



About 190,000 results (0.47 seconds)

[Похищены деньги путем взлома интернет-банка... - Банки.ру](http://www.banki.ru)
www.banki.ru > ... > Отзывы о Абсолют Банке Translate this page
Отзывы о Абсолют Банке, г. Омск. Похищены деньги путем взлома интернет-банка... БЕЗ ОЦЕНКИ. В недавнем прошлом писал, что похитили деньги с ...

[Мошенники взломали программу Сбербанка Онлайн | Банки.ру](http://www.banki.ru/forum/?PAGE_NAME=read&FID=61...)
www.banki.ru/forum/?PAGE_NAME=read&FID=61... Translate this page
Jul 30, 2017 - 25 posts - 10 authors
Здравствуйтесь дорогие пользователи данного сайта. Хочу поделиться историей безразличия СБЕРБАНКА при действиях ...

[Google распространяет программу для взлома "Сбербанка Онлайн ...](http://www.fontanka.ru/2012/12/12/243/)
www.fontanka.ru/2012/12/12/243/ Translate this page
Dec 13, 2012 - Эти пароли банк присылает своему клиенту при проведении транзакций через интернет-банкинг, чтобы исключить возможность ...

[Взлом банка по шагам: шаг первый - «Хакер»](#)
Translate this page
... шаг первый ... Как? Вершина — взлом пентагона. Но это ... открыть тысяч анонимных счетов в web-банках (через

[Научим "взламывать" Интернет-банки. Бесплатно - SecurityLab](http://www.securitylab.ru)
www.securitylab.ru > Блоги > Личные блоги Translate this page
Sep 3, 2012 - Система PHDays I-Bank представляет собой типичный интернет-банк с веб-интерфейсом, процессингом и PIN-кодами для доступа к ...

тыс. историй взлома различных web ресурсов

Инвестиции компаний



- Средства защиты периметра
- Средства защиты веб-приложений и их пользователей

Доли атак



- Атаки на периметр напрямую
- Атаки на периметр через веб-приложения

PT Application Firewall адекватная реакция на вызовы современного Интернета



- Компания Positive Technologies является визионером магического квадранта Gartner по **безопасности веб-приложений**
- Positive Technologies единственная российская Компания, которая представлена в квадранте Gartner с решением данного класса

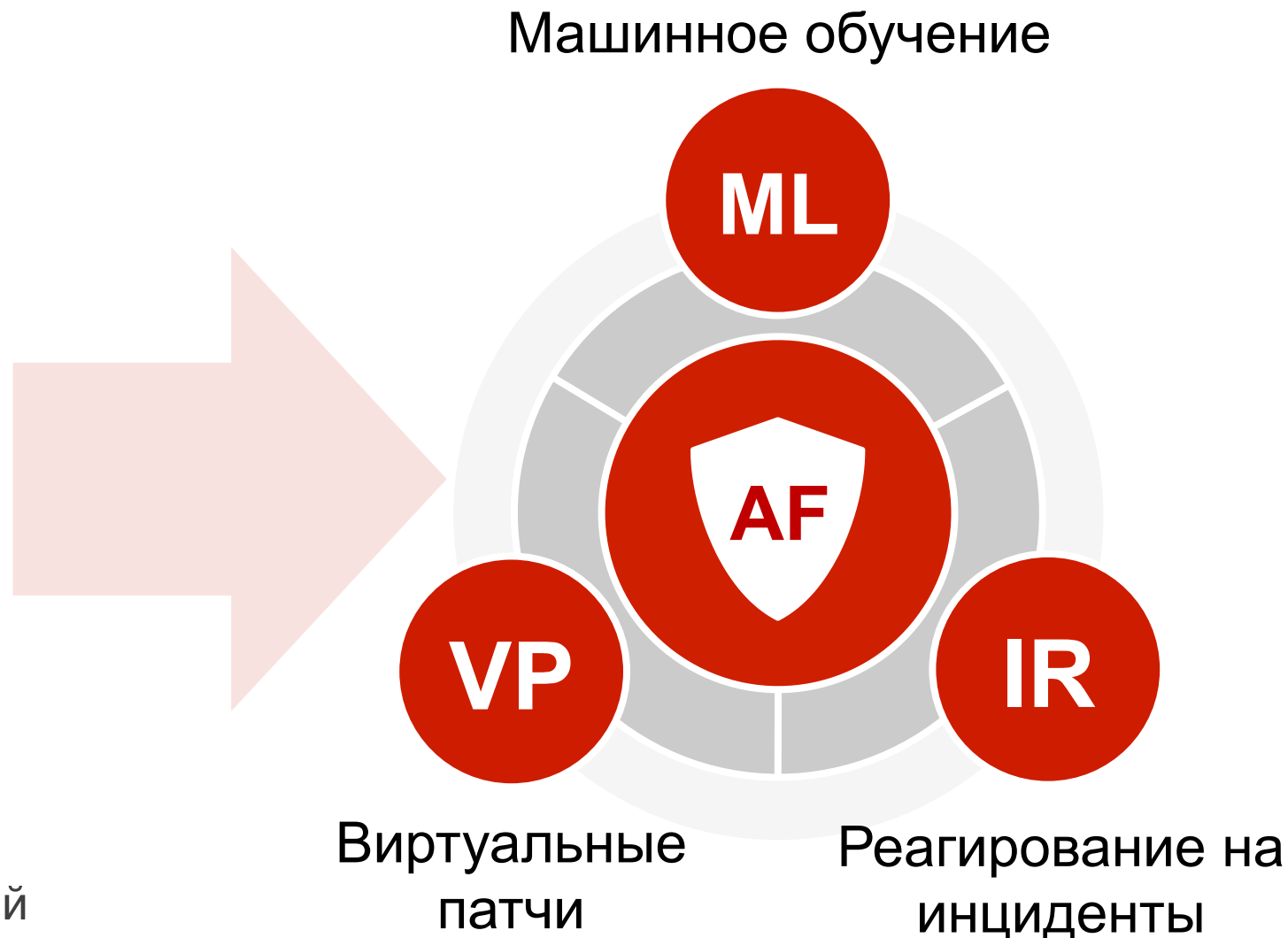
360°
защита

- Web-приложения
- Пользователи
- Бизнес-логика

Позитивная модель – вероятностные алгоритмы для блокирования новых атак

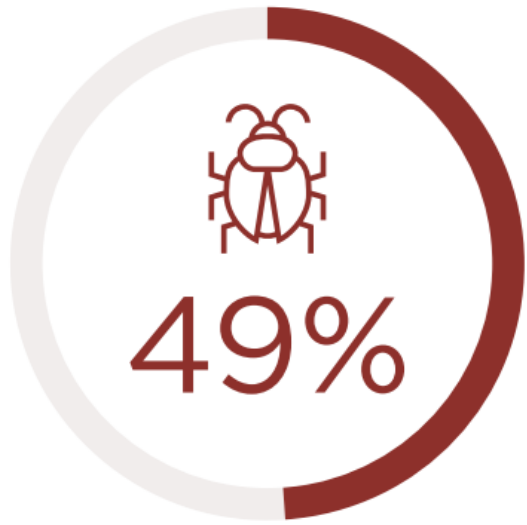
Негативная модель – анализ исходных кодов для исключения возможных угроз до вывода приложения в эксплуатацию

Расследование – корреляционный движок для выявления цепочек атак



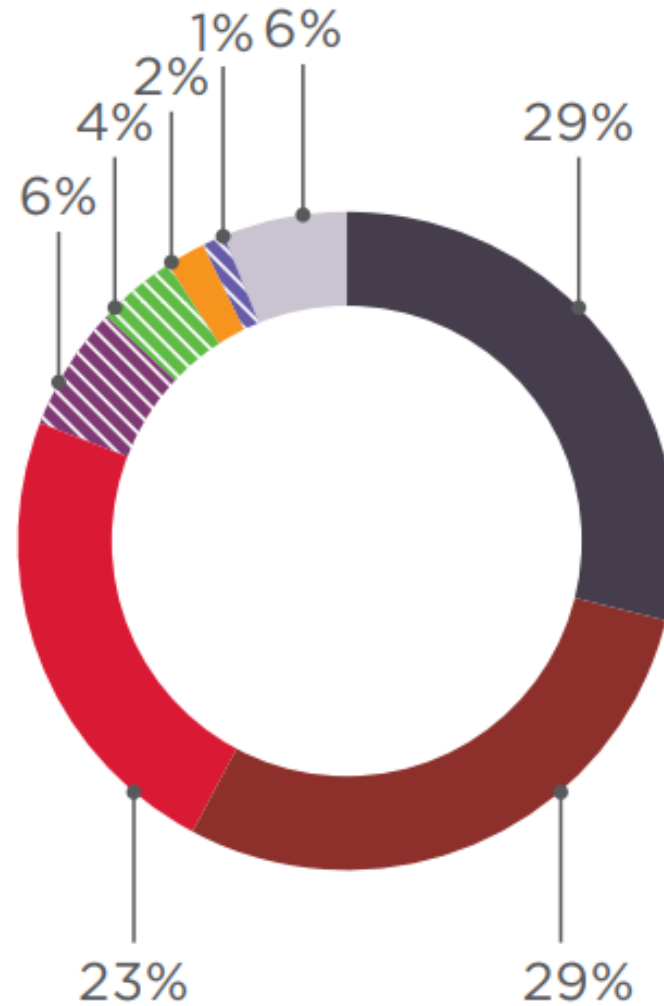
PT MultiScanner

Многопоточная система выявления
вредоносного контента



Шпионское ПО **26%**

ВПО для удаленного управления **22%**



- Компрометация серверов и рабочих станций
- Веб-сайты
- Электронная почта
- Поддельные обновления
- Официальные магазины приложений
- Социальные сети
- Мессенджеры и SMS-сообщения
- Другой



Локализация угроз

Помогает локализовать и предотвратить распространение заражения по всем актуальным каналам в инфраструктуре



Мультивендорный подход

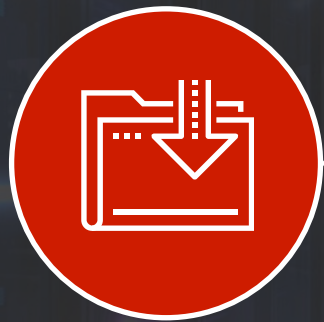
Использует для выявления вредоносного ПО несколько антивирусных движков, статический анализ и черные списки, предоставляемые Positive Technologies



Единая точка мониторинга и хранения объектов

Централизованно анализирует и хранит передаваемые объекты для удобства расследования инцидентов

Ретроспективный анализ объектов позволяет выявлять распределенные во времени атаки и скрытое присутствие ВПО в инфраструктуре



Единое хранилище проанализированных объектов



Неограниченное по времени хранение файлов и метаданных



Автоматическое пересканирование без нагрузки на систему



Пересканирование при обновлении движков и репутационных списков

PT MultiScanner



Защита
почты



Расследование
инцидентов



Контроль
корпоративного
трафика



Внутренний
сервис



Контроль
файловых
хранилищ



Защита
веб-порталов



Контроль
пользовательского
веб-трафика

PT Network Attack Discovery (NAD)

Решение класса Network Forensics, предназначенное для анализа сетевого трафика и расследования инцидентов

- Детализированный разбор более **30** наиболее распространенных протоколов
- Хранение **всего** сырого трафика с разделением на отдельные сессии
- **3000+** собственных сигнатур, качество которых признано мировыми лидерами ET, Cisco Talos
- **Сквозной поиск** по множеству полей протоколов (более 1000)
- Глубокая интеграция с экосистемой **PT: PT MultiScanner, MaxPatrol SIEM**



- Географическая принадлежность IP-адресов, участвующих в сетевом взаимодействии
- Извлеченные файлы и данные, передаваемые по протоколам прикладного уровня
- Определение имен, типов передаваемых файлов и их контрольных сумм
- Сбор информации о баннерах сетевых приложений
- Постоянная индексация в режиме реального времени всего захватываемого сетевого трафика с сохранением в БД полученной информации:
 - время (начало, конец сессии);
 - IP-адреса узлов;
 - протокол транспортного уровня;
 - номера портов;
 - протокол прикладного уровня;
 - объем переданных данных;
 - доменные имена узлов;
 - разобранные поля протоколов прикладного уровня.

Общие сведения

Протоколы	http, tcp
Начало	27 июня 2018, 12:13:00
Конец	27 июня 2018, 12:13:02
Длительность	0 секунд
Отправлено	3 кБ, 49 пакетов
Получено	746 кБ, 505 пакетов
Отправитель	154.179.83.221:34745 ? [AS8452 TE-AS] 🇪🇬 (EG) Египет 00:0C:29:92:67:E1
Получатель	179.241.18.181:80 ? [AS22085 Claro S/A] 🇧🇷 (BR) Бразилия 00:0C:29:79:FD:9E
Хранилище	Challenge
PCAP-файлы	/opt/ptsecurity/data/persistent/48/thread-0/2018-02-19_17/log_2018-02-19.0.1519...

Атаки

- 🔴 [PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain
- 🔴 [PT OPEN] Metasploit MS17-010 ETERNALROMANCE exploitation (CVE-2017-0143)
Attempted Administrator Privilege Gain
- 🔴 [PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain

Еще 1 атака ▾

Файлы

EXE ddd.exe	718.34 кБ
/	↓

Учетные записи

✔ administrator	123456789
-----------------	-----------

HTTP

19.02.18 20:32:06	GET	/ddd.exe 154.179.83.221:34745	0 Б	OK 200	application/x-msdos-program	718.34 кБ UNKNOWN	⤴
----------------------	-----	----------------------------------	-----	-----------	-----------------------------	----------------------	---

Общие сведения

Протоколы [http, tcp](#)


Начало 27 июня 2018, 12:13:00


Конец 27 июня 2018, 12:13:02

Длительность 0 секунд

Отправлено 3 кБ, 49 пакетов

Получено 746 кБ, 505 пакетов

Отправитель [154.179.83.221:34745](#) ⓘ
[AS8452 TE-AS]
 (EG) Египет
[00:0C:29:92:67:E1](#)

Получатель [179.241.18.181:80](#) ⓘ
[AS22085 Claro S/A]
 (BR) Бразилия
[00:0C:29:79:FD:9E](#)

Хранилище [Challenge](#)

PCAP-файлы [/opt/ptsecurity/data/persistent/48/thread-0/2018-02-19_17/log_2018-02-19.0.1519...](#)

Атаки

- [PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain
- [PT OPEN] Metasploit MS17-010 ETERNALROMANCE exploitation (CVE-2017-0143)
Attempted Administrator Privilege Gain
- [PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain

[Еще 1 атака](#) ▾

Файлы

EXE [ddd.exe](#) 718.34 кБ
/ ↓

Учетные записи

✓ administrator 123456789

HTTP

19.02.18 20:32:06	GET	/ddd.exe 154.179.83.221:34745	0 Б	OK 200	application/x-msdos-program	718.34 кБ UNKNOWN	↑
----------------------	-----	--	-----	-----------	-----------------------------	---	---

Общие сведения

Протоколы	http, tcp
Начало	27 июня 2018, 12:13:00
Конец	27 июня 2018, 12:13:02
Длительность	0 секунд
Отправлено	3 кБ, 49 пакетов
Получено	746 кБ, 505 пакетов
Отправитель	154.179.83.221:34745 ? [AS8452 TE-AS] 🇪🇬 (EG) Египет 00:0C:29:92:67:E1
Получатель	179.241.18.181:80 ? [AS22085 Claro S/A] 🇧🇷 (BR) Бразилия 00:0C:29:79:FD:9E
Хранилище	Challenge
PCAP-файлы	/opt/ptsecurity/data/persistent/48/thread-0/2018-02-19_17/log_2018-02-19.0.1519...

Атаки

- [PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain
 - [PT OPEN] Metasploit MS17-010 ETERNALROMANCE exploitation (CVE-2017-0143)
Attempted Administrator Privilege Gain
 - [PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain
- [Еще 1 атака](#) ▾

Файлы

EXE ddd.exe	718.34 кБ
/	↓

Учетные записи

✔ administrator	123456789
-----------------	-----------

HTTP

19.02.18 20:32:06	GET	/ddd.exe 154.179.83.221:34745	0 Б	OK 200	application/x-msdos-program	718.34 кБ UNKNOWN	↑
----------------------	-----	----------------------------------	-----	-----------	-----------------------------	----------------------	---

Общие сведения

Протоколы [http, tcp](#)
Начало 27 июня 2018, 12:13:00
Конец 27 июня 2018, 12:13:02
Длительность 0 секунд
Отправлено 3 кБ, 49 пакетов
Получено 746 кБ, 505 пакетов
Отправитель 154.179.83.221:34745
[AS8452 TE-AS]
 (EG) Египет
00:0C:29:92:67:E1
Получатель 179.241.18.181:80
[AS22085 Claro S/A]
 (BR) Бразилия
00:0C:29:79:FD:9E
Хранилище [Challenge](#)
PCAP-файлы [/opt/ptsecurity/data/persistent/48/thread-0/2018-02-19_17/log_2018-02-19.0.1519...](#)

Атаки

- [PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain
- [PT OPEN] Metasploit MS17-010 ETERNALROMANCE exploitation (CVE-2017-0143)
Attempted Administrator Privilege Gain
- [PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain

[Еще 1 атака](#)

Файлы


ddd.exe	718.34 кБ
/	
Учетные записи	
administrator	123456789


Все файлы скачиваемые

HTTP

19.02.18 20:32:06	GET	/ddd.exe 154.179.83.221:34745	0 Б	OK 200	application/x-msdos-program	718.34 кБ UNKNOWN	
----------------------	-----	----------------------------------	-----	-----------	-----------------------------	----------------------	--

Общие сведения

Протоколы [http, tcp](#)
Начало 27 июня 2018, 12:13:00
Конец 27 июня 2018, 12:13:02
Длительность 0 секунд
Отправлено 3 кБ, 49 пакетов
Получено 746 кБ, 505 пакетов
Отправитель [154.179.83.221:34745](#) ⓘ
[\[AS8452 TE-AS\]](#)
 (EG) Египет
[00:0C:29:92:67:E1](#)

Получатель [179.241.18.181:80](#) ⓘ
[\[AS22085 Claro S/A\]](#)
 (BR) Бразилия
[00:0C:29:79:FD:9E](#)

Хранилище [Challenge](#)
PCAP-файлы [/opt/ptsecurity/data/persistent/48/thread-0/2018-02-19_17/log_2018-02-19.0.1519...](#)

Атаки

- [PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain
- [PT OPEN] Metasploit MS17-010 ETERNALROMANCE exploitation (CVE-2017-0143)
Attempted Administrator Privilege Gain
- [PT OPEN] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)
Attempted Administrator Privilege Gain

[Еще 1 атака](#) ▾

Файлы

EXE [ddd.exe](#) 718.34 кБ
/ ↓

Учетные записи

✓ administrator 123456789

Все файлы скачиваемые

HTTP

19.02.18 20:32:06	GET	/ddd.exe 154.179.83.221:34745	0 Б	OK 200	application/x-msdos-program	718.34 кБ UNKNOWN	↑
----------------------	-----	--	-----	-----------	---	---	---

Логинов Роман
Менеджер по продвижению продуктов
rloginov@ptsecurity.com
+7 903 737 4122

Спасибо за внимание!

POSITIVE TECHNOLOGIES

ptsecurity.ru