



Узнайте, как защититься
от врагов — раскройте
истинный ландшафт угроз
для вашей организации

Ландшафт угроз на Kaspersky Threat Intelligence Portal



Kaspersky Threat Intelligence Portal



Threat Landscape

Пользователи **Kaspersky Threat Intelligence Portal** имеют уникальную возможность составить ландшафт угроз для своей организации в разделе Threat Landscape, специально разработанном для получения информации о злоумышленниках, нацеленных на конкретную отрасль и регион и сочетающем в себе технологии обнаружения с глобальной разведкой угроз. Это позволяет получить полный и актуальный контекст об угрозах, связанных с вашими потенциальными противниками, их тактиками, техниками и процедурами (TTPs).

Ландшафт угроз для вашей организации на Kaspersky Threat Intelligence Portal

Глобальный ландшафт угроз непрерывно меняется: с каждым днем появляются новые способы осуществления атак, а уже известные эволюционируют и становятся все более изощренными. Сегодня командам информационной безопасности все важнее уметь эффективно определять приоритетность угроз, требующих оперативного устранения. Однако, как сосредоточиться на угрозах, которые важны именно для вашего бизнеса, отрасли и региона?

Threat Landscape предоставляет информацию об угрозах, связанных с:



географией



индустрией



типами угроз



преступными группировками



их техниками, тактиками и процедурами (TTPs)



используемым ими ВПО



соответствующими индикаторами компрометации (IoCs)

Разведывательные данные собираются **в режиме реального времени при помощи разнообразных экспертных систем**, используемых в «Лаборатории Касперского» для борьбы с киберпреступностью уже более 25 лет, включая сеть Kaspersky Security Network, позволяющей получать анонимные данные об угрозах от миллионов пользователей по всему миру. Эта же информация используется в продуктах «Лаборатории Касперского», что подтверждается наивысшими баллами в целом ряде независимых тестов и внешних обзоров. Полученные данные тщательно анализируются командами исследователей угроз и обрабатываются современными автоматизированными системами, такими как «песочницы», эвристические движки, инструменты поиска похожих сэмплов, превращаясь в гарантированно проверенную и актуальную информацию.

Принцип работы

Источники Kaspersky Threat Intelligence

Сеть KSN

Сенсоры

Поисковые роботы

Ботофермы

Спам и IoT ловушки

Пассивные DNS

Партнерские сети и OSINT



Анализ

400 000+

сэмплов вредоносных файлов детектируется ежедневно



Kaspersky
Threat Intelligence
Portal



Профили злоумышленников

- Названия / Псевдонимы
- Описания
- Страны / Индустрии
- TTPs
- ВПО / Отчеты



Профили ВПО

- Названия / Псевдонимы
- Описания
- Акторы
- TTPs
- SIGMA-правила



Аналитические отчеты
об угрозах

- YARA, SIGMA, Suricata-правила
- TTPs
- IOCs



Техники, тактики и процедуры (TTP's) MITRE ATT&CK

Threat Landscape



Фильтры

Индустрия

Страна

Акторы

Окружение

Тепловая карта
угроз по MITRE
ATT&CK

Подробные описания TTP's на
основе ежедневного потока
данных вредоносных сэмплов

Статистика ТОП-10:

- TTPs
- ВПО
- Акторы
- Уязвимости
- Индустрии

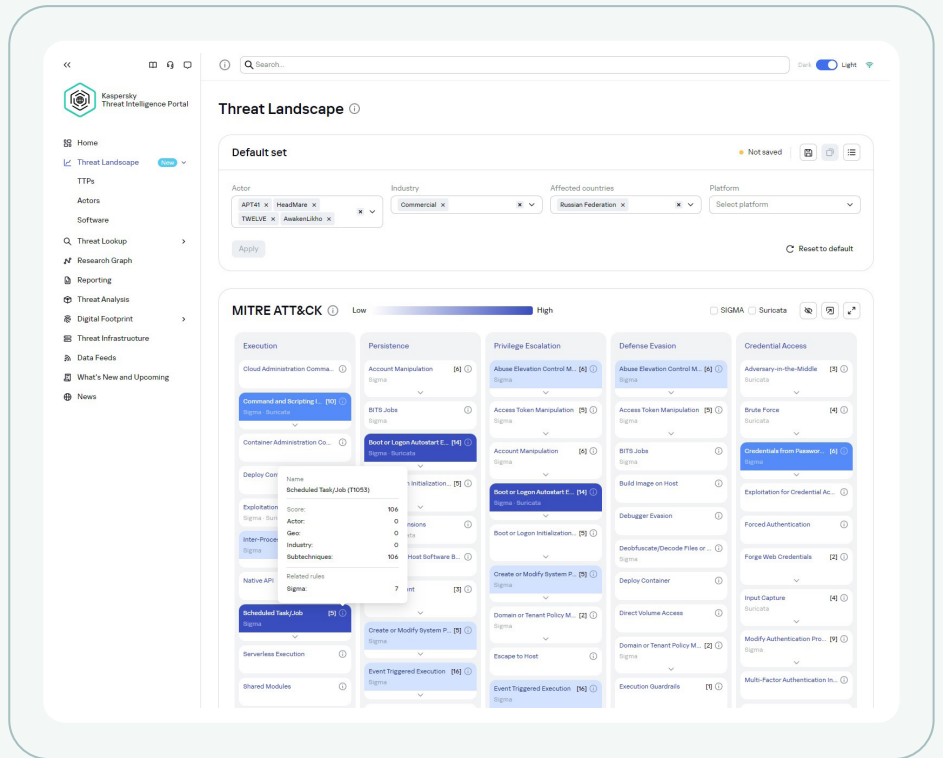
Митигации
(защитные
меры)

Мы ежедневно обрабатываем **сотни тысяч сэмплов вредоносных файлов**, из которых извлекаются данные по геолокации и индустрии, после чего внутренние системы «Лаборатории Касперского» извлекают связанные с ними TTP's и атрибутируют файлы с известными киберпреступными группировками и вредоносным программным обеспечением. Также в основу раздела Threat Landscape заложен поток данных об угрозах, которые поступают от международных команд экспертов «Лаборатории Касперского» в ходе непрерывных расследований.

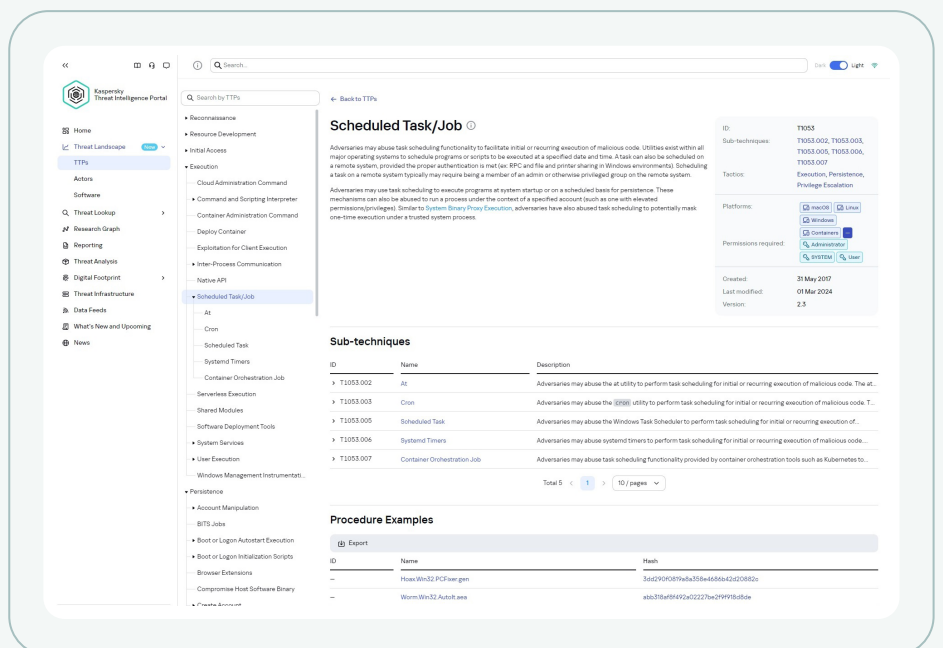
Используя фильтры, пользователи могут получить уникальный ландшафт угроз, основанный на **методологии MITRE ATT&CK**, получив самую актуальную информацию о потенциальных противниках: техниках, тактиках и процедурах, которые наиболее вероятно могут быть применены для осуществления атаки, подробные описания злоумышленников, используемые ими вредоносное программное обеспечение, ознакомиться с отчетами, в которых уже описаны действия этих акторов, а также получить конкретные рекомендации по мерам защиты.

Особенности

Тепловая карта для построения **уникального ландшафта угроз для вашей организации** в режиме реального времени. Применив фильтры, пользователь получает доступ к самым актуальным данным, включая обновления за последние сутки, получаемые нашими системами и экспертами в ходе непрерывных исследований. Возможность сохранения MITRE матриц с различными фильтрами для организаций с филиалами в разных странах или MSSP.



Подробные описания **техник, тактик и процедур злоумышленников** по MITRE ATT&CK.



Подробные описания
процедур, связанных
с техниками.

The screenshot displays the Scepemy Threat Intelligence Portal interface. At the top, there are several detection name cards with dates and severity levels. Below this, a table titled "Related Tactics, Techniques, and Procedures" lists various TTPs. The table has columns for Title, Techniques, Details, and Severity. The details column contains technical information such as registry paths and command-line arguments. A "File signatures and certificates" section at the bottom indicates that no data was found.

Title	Techniques	Details	Severity
TA0005 Persistence	TIS47.004 Winlogon Helper DLL	Change Winlogon Helper DLL via Registry [Image_path] "Bundlr\winnt.exe" "Registry_key" "REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" "Registry_value" "Explore.exe" "Registry_value_name" "Shell"	High
TA0005 Persistence	TIS47.004 Winlogon Helper DLL	Change Winlogon Helper DLL via Registry [Image_path] "Bundlr\winnt.exe" "Registry_key" "REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" "Registry_value" "Explore.exe" "Registry_value_name" "Shell"	High
TA0005 Persistence	TIS47.004 Winlogon Helper DLL	Change Winlogon Helper DLL via Registry [Image_path] "Bundlr\winnt.exe" "Registry_key" "REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" "Registry_value" "Explore.exe" "Registry_value_name" "Shell"	High
TA0005 Persistence	TIS47.004 Winlogon Helper DLL	Change Winlogon Helper DLL via Registry [Image_path] "Bundlr\winnt.exe" "Registry_key" "REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" "Registry_value" "Explore.exe" "Registry_value_name" "Shell"	High
TA0004 Privilege Escalation	TIS47.004 Winlogon Helper DLL	Change Winlogon Helper DLL via Registry [Image_path] "Bundlr\winnt.exe" "Registry_key" "REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" "Registry_value" "Explore.exe" "Registry_value_name" "Shell"	High
TA0004 Privilege Escalation	TIS47.004 Winlogon Helper DLL	Change Winlogon Helper DLL via Registry [Image_path] "Bundlr\winnt.exe" "Registry_key" "REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" "Registry_value" "Explore.exe" "Registry_value_name" "Shell"	High
TA0004 Privilege Escalation	TIS47.004 Winlogon Helper DLL	Change Winlogon Helper DLL via Registry [Image_path] "Bundlr\winnt.exe" "Registry_key" "REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" "Registry_value" "Explore.exe" "Registry_value_name" "Shell"	High
TA0004 Privilege Escalation	TIS47.004 Winlogon Helper DLL	Change Winlogon Helper DLL via Registry [Image_path] "Bundlr\winnt.exe" "Registry_key" "REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" "Registry_value" "Explore.exe" "Registry_value_name" "Shell"	High
TA0005 Defense Evasion	TIR2 Modify Registry	Change Winlogon Helper DLL via Registry [Image_path] "Bundlr\winnt.exe" "Registry_key" "REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" "Registry_value" "Explore.exe" "Registry_value_name" "Shell"	High
TA0005 Defense Evasion	TIR2 Modify Registry	Change Winlogon Helper DLL via Registry [Image_path] "Bundlr\winnt.exe" "Registry_key" "REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" "Registry_value" "Explore.exe" "Registry_value_name" "Shell"	High

Доступ к самому обширному
репозиторию профилей
злоумышленников
и вредоносных программ
и с подробными описаниями,
составленными нашими
экспертами.

The screenshot shows the profile page for the "AwakenLiko" group in the Scepemy Threat Intelligence Portal. The page includes a header with the group name, a "Back to Actions" button, and a "Details" section with fields for ID (A0883), Title (Software), and a "Threats by impact" button. Below this is a "Description" section with text about the group's activities and a "See more" link. At the bottom, there is a world map titled "Affected countries" with a legend listing countries: Australia, Brazil, China, Canada, Germany, India, Japan, South Korea, and Mexico.

Доступ к **Sigma / Yara / Suricata-правилам**, связанным с техниками, тактиками и процедурами по матрице MITRE ATT&CK для обнаружения актуальных для вашей организации угроз.

The screenshot displays the Kaspersky Threat Intelligence Portal interface. On the left, a navigation menu lists various categories like Threat Landscape, TTPs, Actors, Software, and Threat Lookups. The main content area is titled 'Search by TTPs' and lists several categories such as Cloud Storage Object Discovery, Container and Resource Discovery, and Debugger Evasion. A 'Procedure Examples' table is visible, listing items with columns for ID, Name, and Hash. Below this, a 'Rules' section shows a table with columns for ID, Title, Description, and Severity, listing rules like 'System Owner/User Discovery via PowerShell'.

Статистика по **ТОП-10** индустриям, акторам, TTPs, уязвимостям и ВПО.

The screenshot shows a dashboard with several charts and tables. At the top, there are two charts: 'Top Techniques' (a radar chart with points for T1547, T1548, T1549, T1550, T1551, T1552) and 'Attacks by industry' (a pie chart showing segments for Agriculture, Retail, Manufacturing, Education, and Technology). Below these is a 'Sigma, Suricata, Reports' section with a donut chart showing 45 total items, broken down into Sigma (10), Suricata (15), and Reports (20). Further down are 'Top Software' and 'Top Tactics' sections, each with horizontal bar charts. The 'Top Software' chart lists Cheat, Ngrok, Minikube, and Puget. The 'Top Tactics' chart lists Reconnaissance and Initial Access.



В современном постоянно развивающемся мире киберугроз сегодня присутствуют огромные массивы **данных Threat Intelligence**, доступных через разнообразные продукты и сервисы. Быстро получив доступ к данным об угрозах, актуальных для конкретной организации или конкретного ее филиала, организации могут предпринять правильные шаги для проактивной защиты от соответствующих атак.

Преимущества от использования

Проактивный подход к защите

Понимание наиболее вероятных для организации векторов атак с целью выстроить эффективную защитную стратегию

Мониторинг поверхности атаки

Выявление пробелов в системах безопасности до того, как ими воспользуются злоумышленники

Фокус на релевантных угрозах

Возможность сосредоточиться на угрозах, которые наиболее вероятны для вашего бизнеса, отрасли и региона

Стратегическое планирование

Использование информации о ландшафте угроз при планировании инвестиций и развитии средств / методов защиты

Повышение эффективности подразделений ИБ

Повышение эффективности работы персонала и сокращение затрат на него за счет доступа к информации о релевантных угрозах и мировых тенденциях

Информированность

Осведомленность о самых последних угрозах и их мировых тенденциях для эффективной защиты



Если ты знаешь врага и знаешь себя, тебе не нужно волноваться за исход сотни сражений. Если ты знаешь себя, но не знаешь врага, за каждую достигнутую тобой победу ты расплатишься поражением. Если ты не знаешь ни себя, ни врага, ты будешь проигрывать всегда.

Сунь-Цзы

«Искусство Войны»

Kaspersky Threat Intelligence

«Лаборатория Касперского» предлагает сервисы информирования об угрозах, которые открывают доступ к различной информации, полученной нашими аналитиками и исследователями мирового класса. Эти данные помогут любой организации эффективно противостоять современным киберугрозам.

Наша компания обладает глубокими знаниями, богатым опытом исследования киберугроз и уникальными сведениями обо всех аспектах IT-безопасности. Наша компания обладает глубокими знаниями, богатым собственным опытом исследований киберугроз и уникальными сведениями обо всех аспектах информационной безопасности. Благодаря этому «Лаборатория Касперского» стала доверенным партнером правоохранительных и государственных организаций по всему миру, в том числе Международной организации уголовной полиции ИНТЕРПОЛ и подразделений CERT. Kaspersky Threat Intelligence предоставляет актуальные тактические, операционные и стратегические данные об угрозах.



Kaspersky Threat Intelligence

[Подробнее](#)

www.kaspersky.ru

© 2024 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

[#kaspersky](#)
[#активируйбудущее](#)