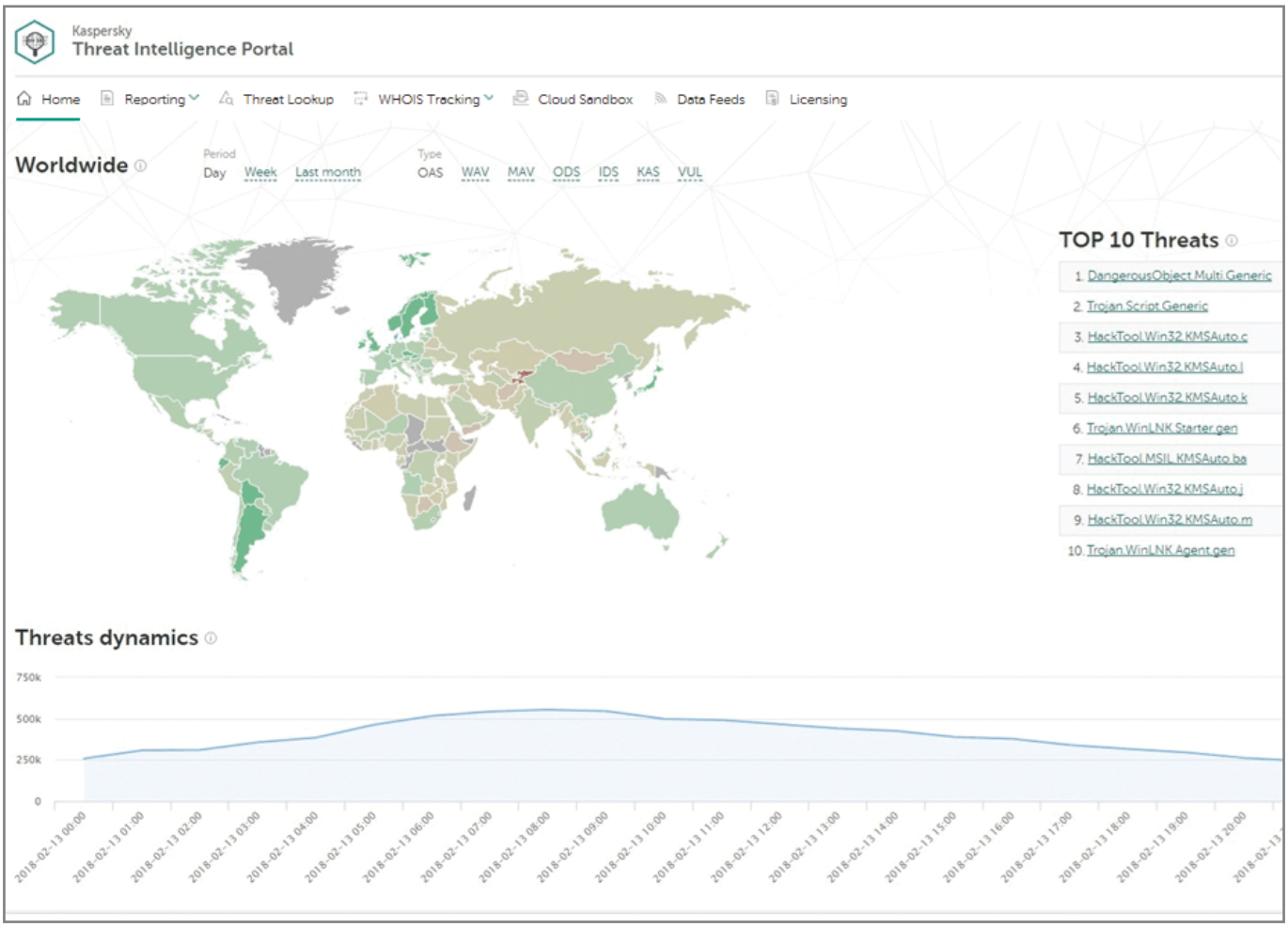
KASPERSKY lab

Портал Kaspersky Threat Intelligence: расследование инцидентов и реагирование на них

www.kaspersky.ru/enterprise
#истиннаябезопасность

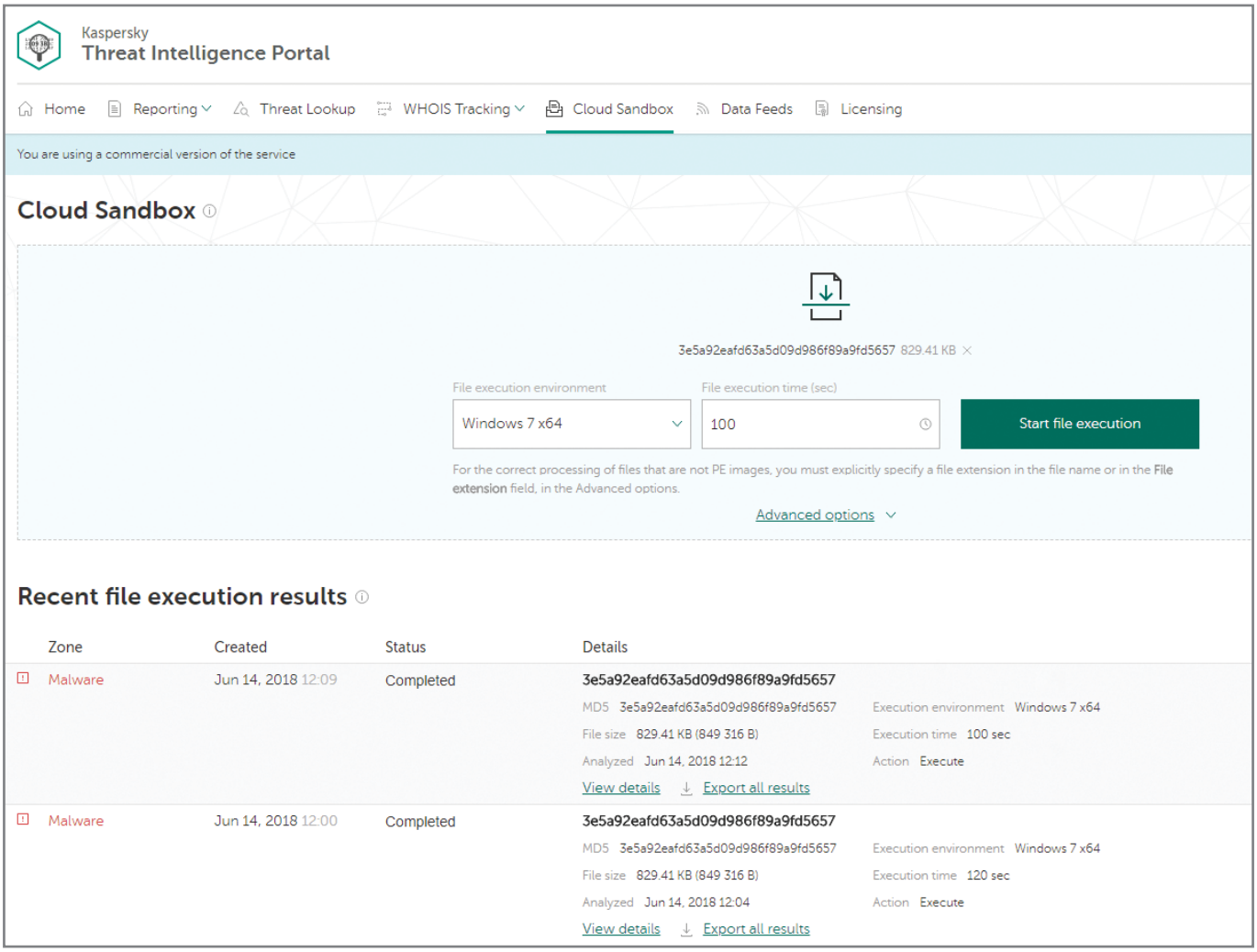
Портал Kaspersky Threat Intelligence предоставляет доступ ко всем знаниям, которые на протяжении более 20 лет собирали, проверяли и классифицировали специалисты «Лаборатории Касперского». Платформа предоставляет подробные и актуальные сведения об угрозах (файлы, URL-адреса, домены, IP-адреса, контрольные суммы файлов, названия угроз, статистику и информацию об активности, данные WHOIS/DNS и т. д.), которые позволяют специалистам по реагированию на инциденты:

- определять, требует ли событие в очереди немедленного реагирования или дополнительного исследования;
- использовать первое обнаружение в качестве исходной точки для раскрытия всех деталей инцидента и соответствующего реагирования;
- определять, на какие системы и как именно повлиял инцидент, – и предоставлять ценную информацию другим вовлеченным отделам;
- изучать тактику и технологии киберпреступников и выявлять их цели для определения максимально эффективных мер противодействия.

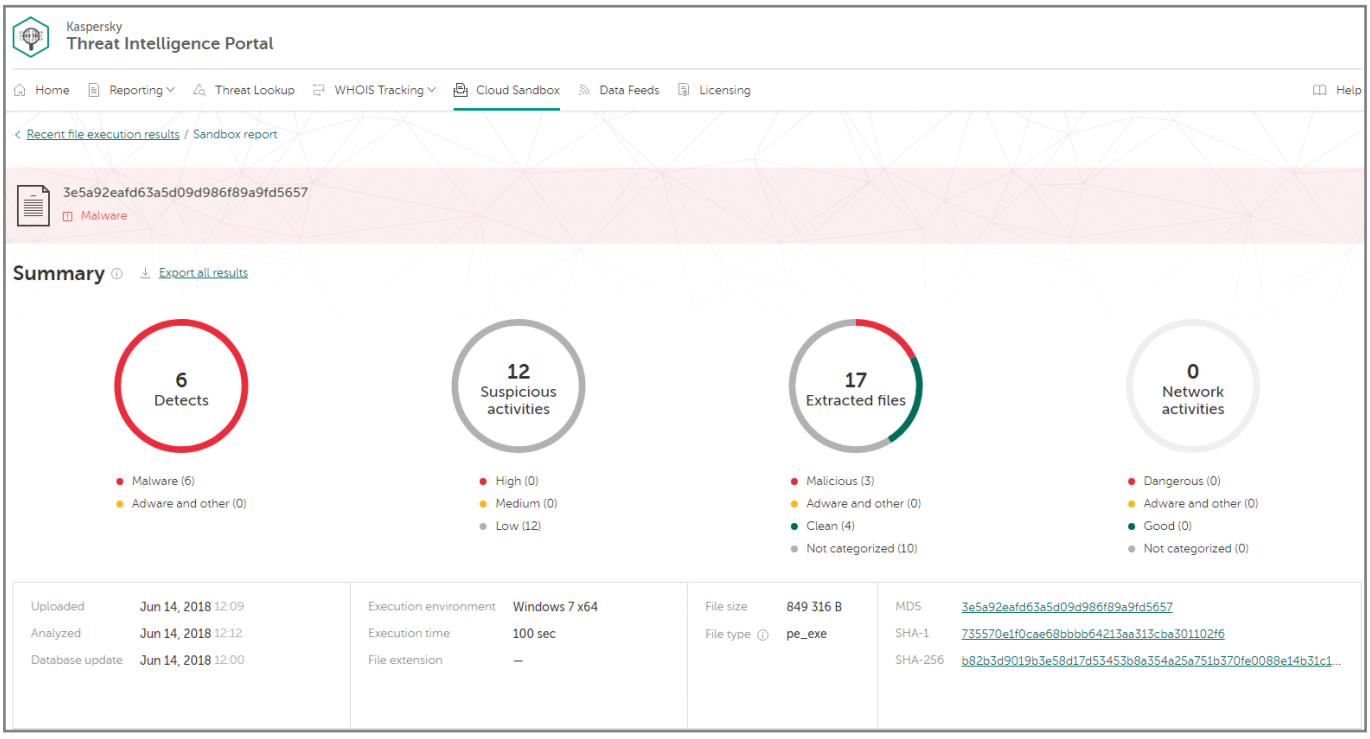


Портал Threat Intelligence содержит множество вкладок, но при рассмотрении данного примера представим, что у нас есть реальные улики. Группа реагирования на инциденты получила образец подозрительного файла, который по окончании рабочего дня инициировал передачу данных из сетевого периметра на внешний IP-адрес. В этом случае можно сразу перейти к вкладке Cloud Sandbox в верхнем меню.

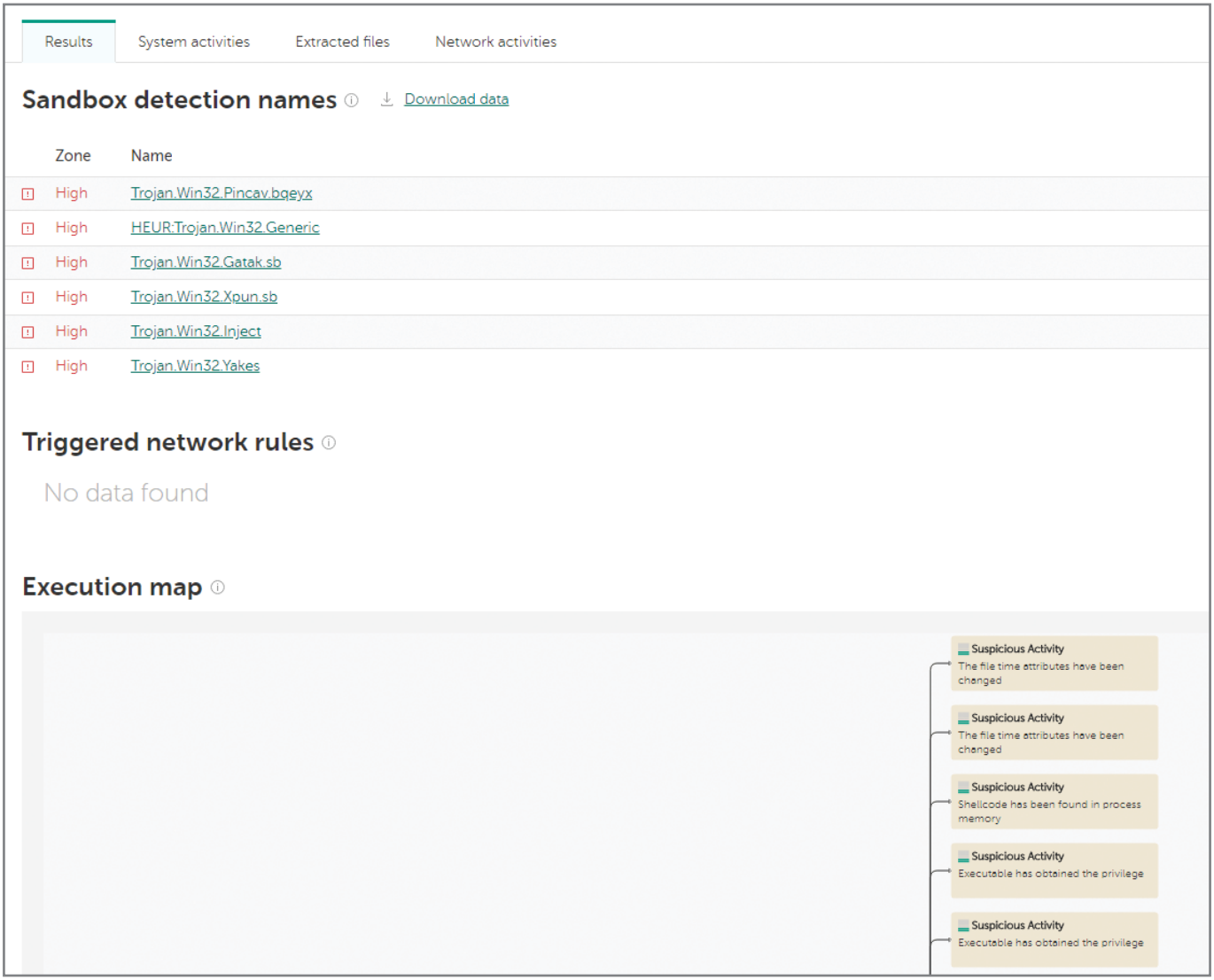
Песочница выполняет подозрительный объект на виртуальной машине с полнофункциональной ОС. Поведение объекта анализируется для выявления его вредоносных действий. Виртуальные машины изолированы от реальной инфраструктуры компании, поэтому запуск не нанесет вреда. Просто выгрузите файл, выберите среду (в данном случае Windows 7), время (допустим, 100 секунд) и запустите выполнение.

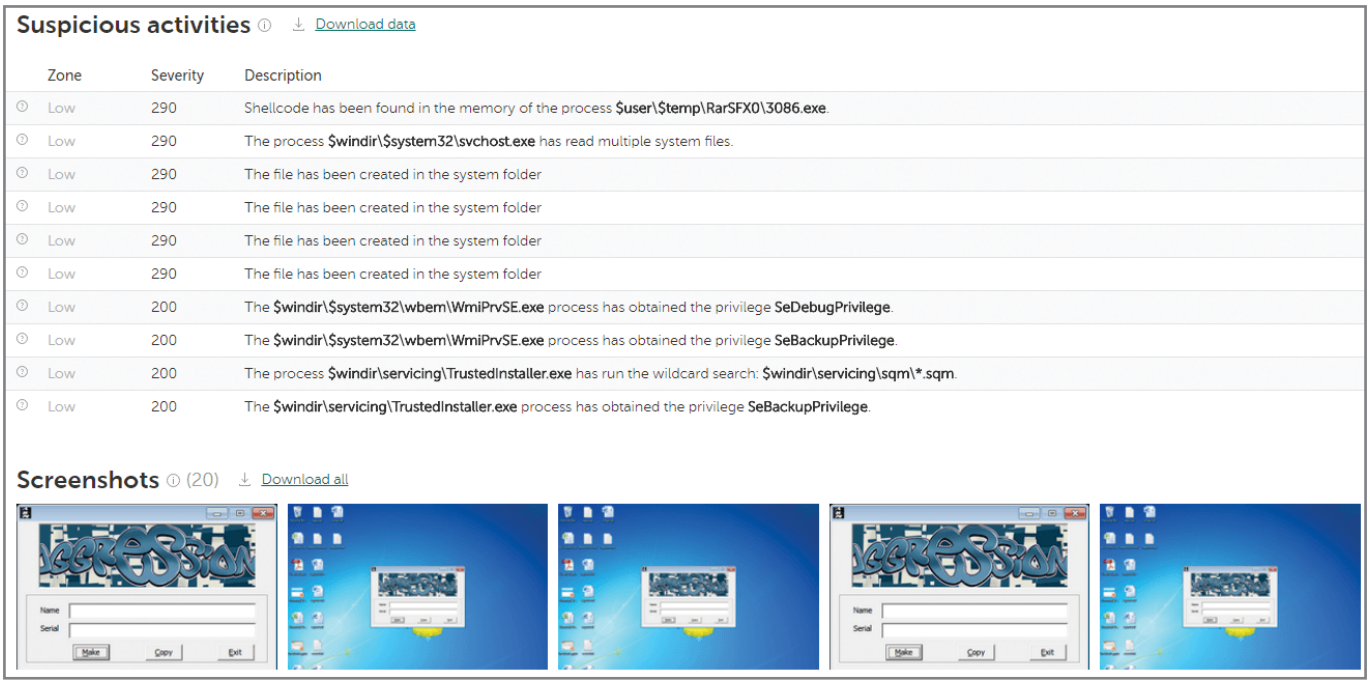


Песочницы эффективно справляются с вредоносным ПО, которое уклоняется от статического анализа и может полностью исчезать из поля зрения антивирусной программы. Даже если большинство антивирусных систем идентифицируют файл как «плохой», они не смогут прояснить степень его вредоносности или фактическое воздействие. Для получения дополнительных сведений посмотрим, что происходит в песочнице «Лаборатории Касперского» после запуска.



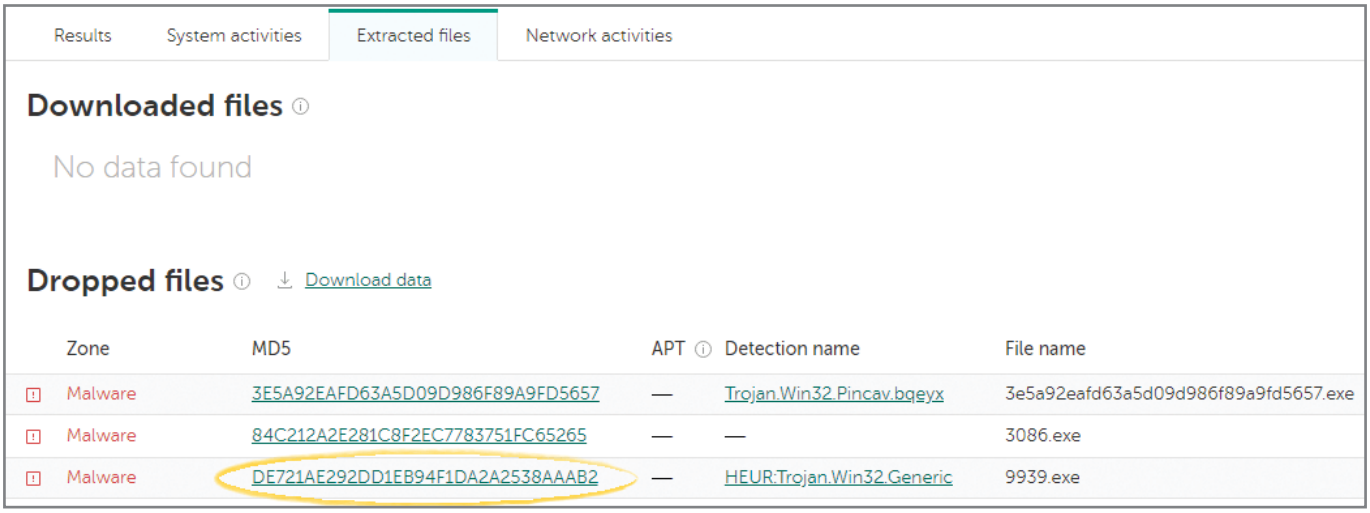
При выполнении тестируемого объекта песочница собирает артефакты, анализирует их и выносит решение. Вот сводные данные: детекты (6), подозрительные действия (12), извлеченные файлы (17) и сетевая активность (0). Этот файл не просто «плохой»: он совершает множество подозрительных действий, и все они перечислены во вкладке.





Специалист по реагированию на инциденты может ознакомиться со снимками экрана, сделанными во время выполнения, на вкладке «Результаты». В некоторых случаях вредоносная программа пытается избежать автоматического анализа, дожидаясь взаимодействия с пользователем (ввода пароля, прокрутки документа, перемещения мыши и т. д.). Облачной песочнице «Лаборатории Касперского» известно множество методов обхода. Для противодействия им используются технологии моделирования поведения человека. Снимки экрана также полезны: исследователь может взглянуть на происходящее в «пробирке» с человеческой точки зрения.

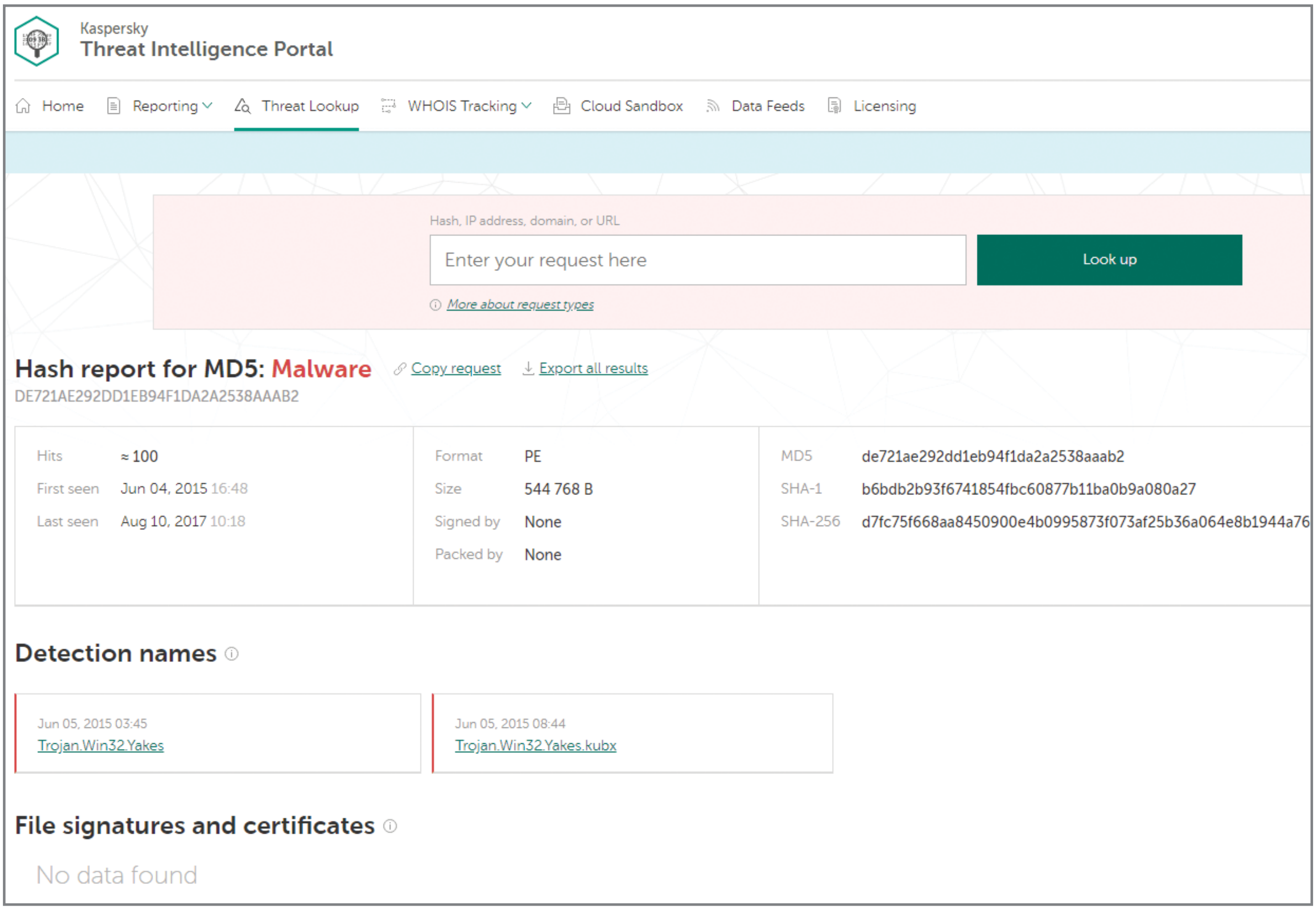
Перейдем на вкладку «Извлеченные файлы», чтобы увидеть, какие объекты были загружены, извлечены или созданы. В нашем случае был отправлен вредоносный файл.



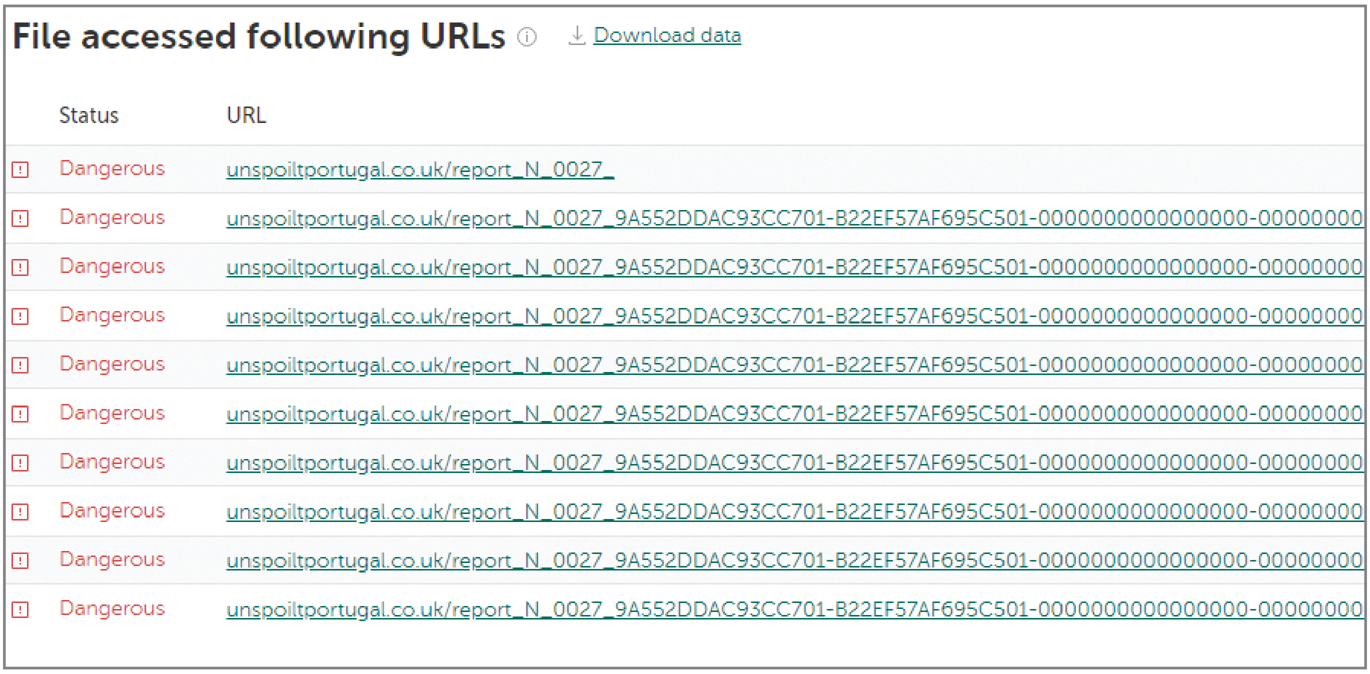
Возможности классической песочницы исчерпались бы на этом этапе: вы выполняете файл, получаете список вредоносных действий – и на этом все. Но при использовании портала Kaspersky Threat Intelligence можно сразу перейти к сервису Threat Lookup для получения более подробных аналитических данных об индикаторах компрометации и их взаимосвязях.

Threat Lookup – это поисковая ИБ-система. Этот сервис содержит более 5 петабайт аналитических данных об угрозах, собранных и классифицированных «Лабораторией Касперского» за последние 20 лет: контрольные суммы файлов, статистические/поведенческие данные, данные WHOIS/DNS, URL-адреса, IP-адреса и т. д.

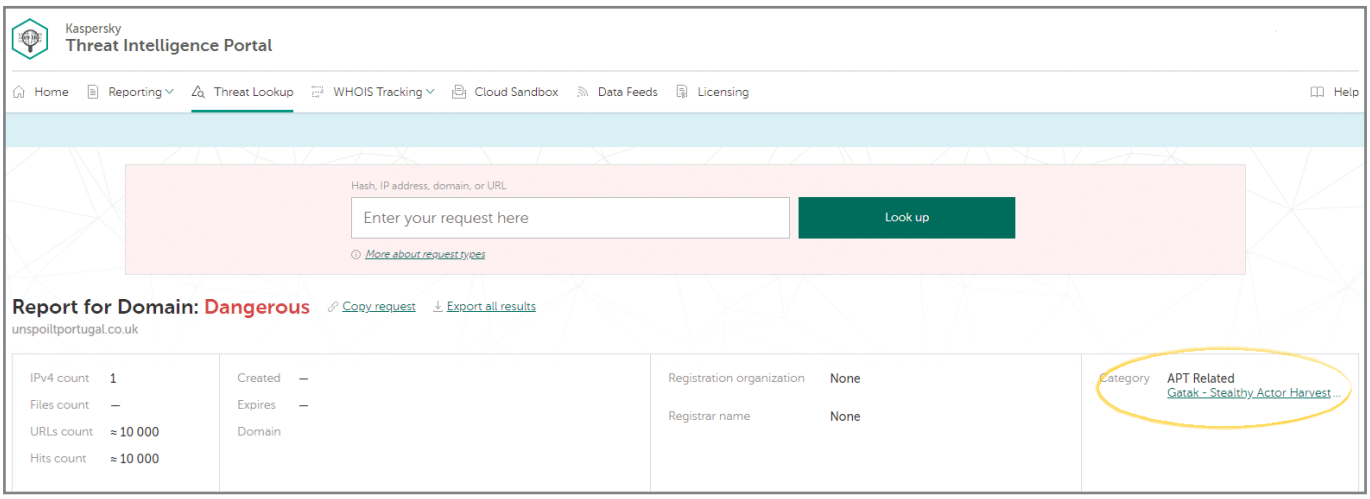
После выполнения образца в песочнице полученные результаты сразу используются в качестве поисковых запросов для сервиса Threat Lookup – достаточно просто кликнуть объект (в данном случае это контрольная сумма MD5).



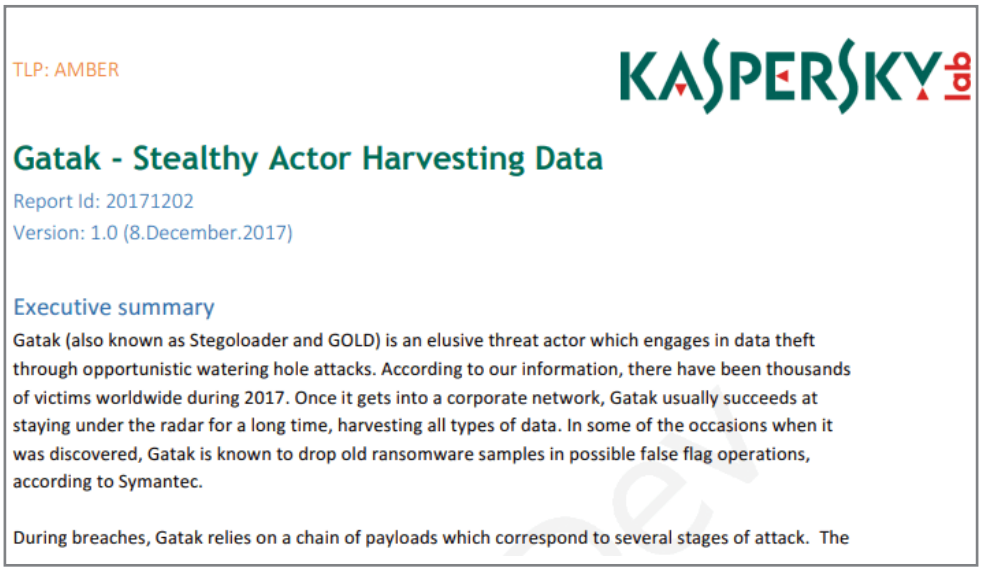
Теперь доступен более подробный отчет о вредоносном ПО. Просмотрим предоставленные Threat Lookup результаты, чтобы увидеть, к каким URL-адресам обращалась вредоносная программа:



Здесь есть URL-адреса, отмеченные как «опасные». Рассмотрим подробнее такой вредоносный URL-адрес, чтобы узнать, какие данные о нем имеются в Threat Lookup:



Выясняется, что исследуемый URL-адрес связан с APT-атакой! Портал Kaspersky Threat Intelligence предлагает загрузить отчет об этой атаке. Этот PDF-файл содержит краткое резюме, детальные технические подробности и список связанных индикаторов компрометации. С ним полезно ознакомиться, чтобы узнать, не происходило ли что-то подобное в вашей организации, и своевременно разработать конкретные сценарии для обнаружения описанной атаки.


TLP: AMBER

KASPERSKY lab

Gatak - Stealthy Actor Harvesting Data

Report Id: 20171202
Version: 1.0 (8.December.2017)

Executive summary

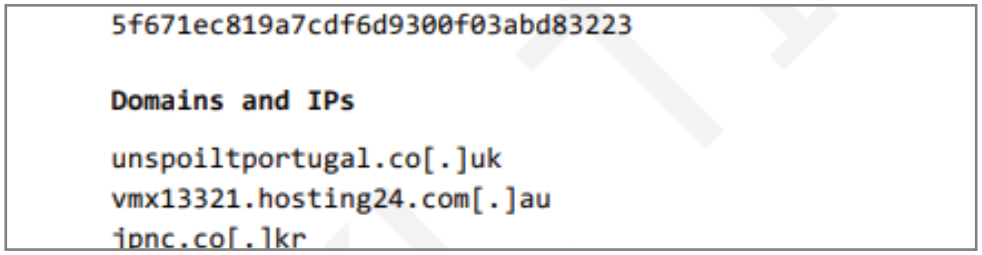
Gatak (also known as Stegoloader and GOLD) is an elusive threat actor which engages in data theft through opportunistic watering hole attacks. According to our information, there have been thousands of victims worldwide during 2017. Once it gets into a corporate network, Gatak usually succeeds at staying under the radar for a long time, harvesting all types of data. In some of the occasions when it was discovered, Gatak is known to drop old ransomware samples in possible false flag operations, according to Symantec.

During breaches, Gatak relies on a chain of payloads which correspond to several stages of attack. The


Appendix I - Indicators of compromise

Stage 0 hashes

0AE26BA127904EC354F228B316F044A1
0B20B941D2B9372D875410FFEB53C473


5f671ec819a7cdf6d9300f03abd83223

Domains and IPs

unspoiltportugal.co[.]uk
vmx13321.hosting24.com[.]au
jpnc.co[.]kr

Портал Kaspersky Threat Intelligence обеспечивает:

- Улучшение и ускорение расследования и реагирования на инциденты. Команды ИБ или SOC получает ценную информацию об угрозах, а также результаты глобальных исследований источников целевых атак. Это позволяет диагностировать и анализировать инциденты безопасности на хостах и в сети более эффективно, а также приоритизировать сигналы внутренних систем о неизвестных угрозах, сводя к минимуму время реагирования на инциденты и предотвращая компрометацию критически важных систем и данных.

- Глубокий поиск индикаторов угроз, таких как IP- и URL-адреса, домены и контрольные суммы файлов, предоставляемые в проверенном контексте связанных с ними угроз, позволяющем приоритизировать атаки, оптимально распределять сотрудников и ресурсы и устранять в первую очередь те угрозы, которые представляют наибольшую потенциальную.опасность для вашей организации.

- Защита от целевых атак. Тактические и стратегические данные об угрозах позволяют усовершенствовать защитные механизмы, адаптируя стратегию безопасности для противодействия конкретным угрозам для вашей организации.

www.kaspersky.ru

#ИстиннаяБезопасность