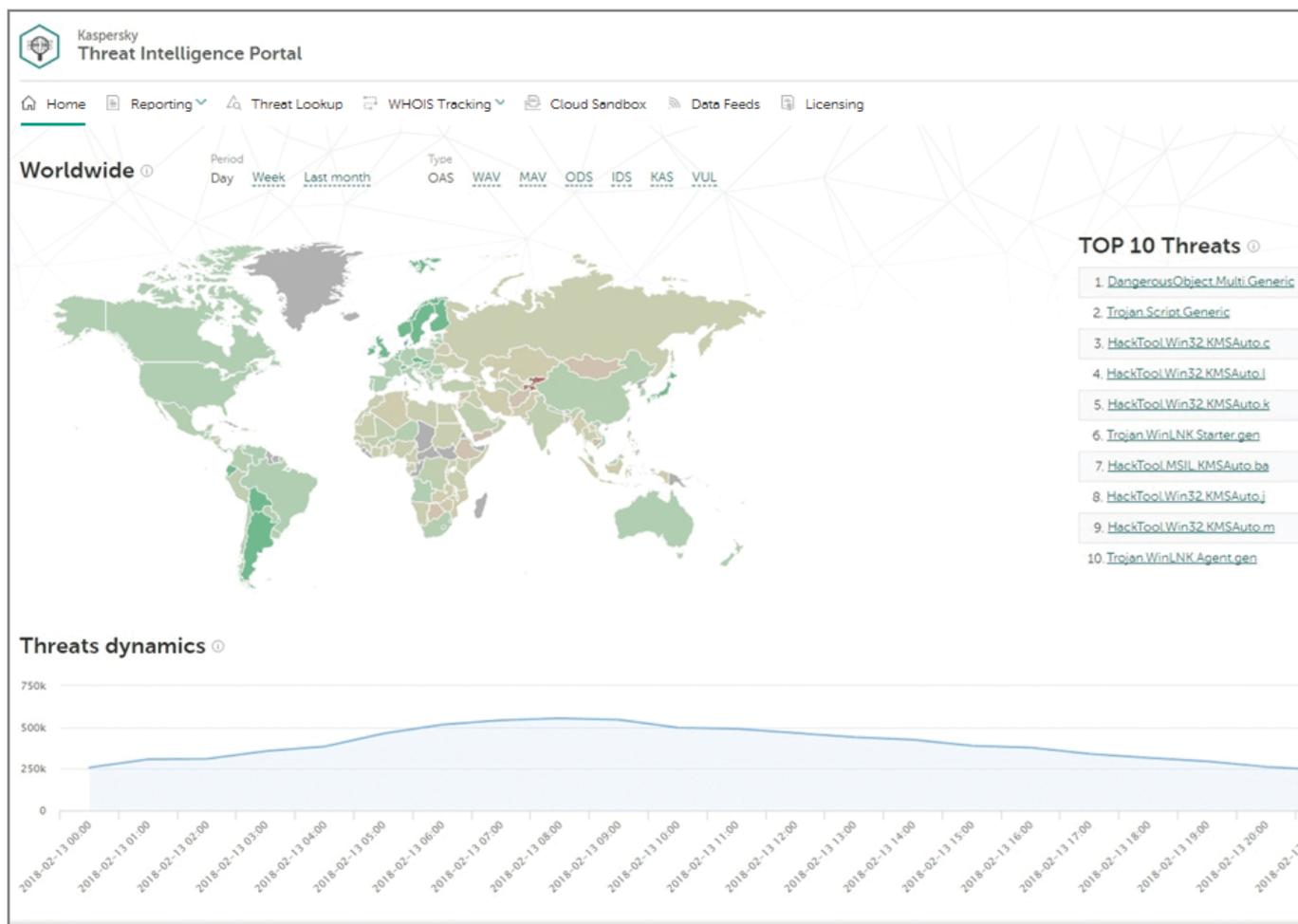


Портал Kaspersky Threat Intelligence: расследование инцидентов и реагирование на них

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.

Kaspersky Threat Intelligence Portal

Home Reporting Threat Lookup WHOIS Tracking Cloud Sandbox Data Feeds Licensing

You are using a commercial version of the service

Cloud Sandbox

3e5a92eafd63a5d09d986f89a9fd5657 829.41 KB

File execution environment: Windows 7 x64 | File execution time (sec): 100

[Start file execution](#)

For the correct processing of files that are not PE images, you must explicitly specify a file extension in the file name or in the File extension field, in the Advanced options.

[Advanced options](#)

Recent file execution results

| Zone | Created | Status | Details |
|---------|--------------------|-----------|--|
| Malware | Jun 14, 2018 12:09 | Completed | 3e5a92eafd63a5d09d986f89a9fd5657 MD5 3e5a92eafd63a5d09d986f89a9fd5657 Execution environment Windows 7 x64 File size 829.41 KB (849 316 B) Execution time 100 sec Analyzed Jun 14, 2018 12:12 Action Execute View details Export all results |
| Malware | Jun 14, 2018 12:00 | Completed | 3e5a92eafd63a5d09d986f89a9fd5657 MD5 3e5a92eafd63a5d09d986f89a9fd5657 Execution environment Windows 7 x64 File size 829.41 KB (849 316 B) Execution time 120 sec Analyzed Jun 14, 2018 12:04 Action Execute View details Export all results |

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.

Kaspersky Threat Intelligence Portal

Home Reporting Threat Lookup WHOIS Tracking Cloud Sandbox Data Feeds Licensing Help

< Recent file execution results / Sandbox report

3e5a92eafd63a5d09d986f89a9fd5657 Malware

Summary

[Export all results](#)

| | | | |
|---|---|---|---|
| <p>6 Detects</p> <ul style="list-style-type: none"> Malware (6) Adware and other (0) | <p>12 Suspicious activities</p> <ul style="list-style-type: none"> High (0) Medium (0) Low (12) | <p>17 Extracted files</p> <ul style="list-style-type: none"> Malicious (3) Adware and other (0) Clean (4) Not categorized (10) | <p>0 Network activities</p> <ul style="list-style-type: none"> Dangerous (0) Adware and other (0) Good (0) Not categorized (0) |
|---|---|---|---|

| | | | |
|-------------------------------------|--------------------------------------|----------------------|---|
| Uploaded: Jun 14, 2018 12:09 | Execution environment: Windows 7 x64 | File size: 849 316 B | MD5: 3e5a92eafd63a5d09d986f89a9fd5657 |
| Analyzed: Jun 14, 2018 12:12 | Execution time: 100 sec | File type: pe_exe | SHA-1: 735570e1f0cae68bbb64213aa313cba301102f6 |
| Database update: Jun 14, 2018 12:00 | File extension: - | | SHA-256: b92b3d9019b3e58d17d53453b8a354a25a751b370fe0088e14b31c1... |

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.

Results System activities Extracted files Network activities

Sandbox detection names [Download data](#)

| Zone | Name |
|------|---|
| High | Trojan.Win32.Pincav.bqeyx |
| High | HEUR:Trojan.Win32.Generic |
| High | Trojan.Win32.Gatak.sb |
| High | Trojan.Win32.Xpoun.sb |
| High | Trojan.Win32.Inject |
| High | Trojan.Win32.Yakes |

Triggered network rules [Download data](#)

No data found

Execution map [Download data](#)

- Suspicious Activity: The file time attributes have been changed
- Suspicious Activity: The file time attributes have been changed
- Suspicious Activity: Shellcode has been found in process memory
- Suspicious Activity: Executable has obtained the privilege
- Suspicious Activity: Executable has obtained the privilege

Suspicious activities [Download data](#)

| Zone | Severity | Description |
|------|----------|--|
| Low | 290 | Shellcode has been found in the memory of the process \$user\temp\RarSFX0\3086.exe. |
| Low | 290 | The process \$windir\system32\svchost.exe has read multiple system files. |
| Low | 290 | The file has been created in the system folder |
| Low | 290 | The file has been created in the system folder |
| Low | 290 | The file has been created in the system folder |
| Low | 290 | The file has been created in the system folder |
| Low | 200 | The \$windir\system32\wbem\WmiPrvSE.exe process has obtained the privilege SeDebugPrivilege. |
| Low | 200 | The \$windir\system32\wbem\WmiPrvSE.exe process has obtained the privilege SeBackupPrivilege. |
| Low | 200 | The process \$windir\servicing\TrustedInstaller.exe has run the wildcard search: \$windir\servicing\sqm*.sqm. |
| Low | 200 | The \$windir\servicing\TrustedInstaller.exe process has obtained the privilege SeBackupPrivilege. |

Screenshots [Download all](#)

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.

| Results | | System activities | | Extracted files | | Network activities | |
|--|--|-------------------|---|--------------------------------------|--|--------------------|--|
| Downloaded files ⓘ | | | | | | | |
| No data found | | | | | | | |
| Dropped files ⓘ Download data | | | | | | | |
| Zone | MD5 | APT ⓘ | Detection name | File name | | | |
| Malware | 3E5A92EAFD63A5D09D986F89A9FD5657 | — | Trojan.Win32.Pincav.bqeyx | 3e5a92eafd63a5d09d986f89a9fd5657.exe | | | |
| Malware | 84C212A2E281C8F2EC7783751FC65265 | — | — | 3086.exe | | | |
| Malware | DE721AE292DD1EB94F1DA2A2538AAAB2 | — | HEUR:Trojan.Win32.Generic | 9939.exe | | | |

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).



Hash, IP address, domain, or URL

Enter your request here

Look up

[More about request types](#)

Hash report for MD5: **Malware** [Copy request](#) [Export all results](#)

DE721AE292DD1EB94F1DA2A2538AAAB2

| | | | | | |
|------------|--------------------|-----------|-----------|---------|--|
| Hits | ≈ 100 | Format | PE | MD5 | de721ae292dd1eb94f1da2a2538aaab2 |
| First seen | Jun 04, 2015 16:48 | Size | 544 768 B | SHA-1 | b6bdb2b93f6741854fbc60877b11ba0b9a080a27 |
| Last seen | Aug 10, 2017 10:18 | Signed by | None | SHA-256 | d7fc75f668aa8450900e4b0995873f073af25b36a064e8b1944a76 |
| | | Packed by | None | | |

Detection names

| | |
|--|---|
| Jun 05, 2015 03:45 Trojan.Win32.Yakes | Jun 05, 2015 08:44 Trojan.Win32.Yakes.kubx |
|--|---|

File signatures and certificates

No data found

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

File accessed following URLs [Download data](#)

| Status | URL |
|-----------|---|
| Dangerous | unspoilportugal.co.uk/report_N_0027_ |
| Dangerous | unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000 |

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

The screenshot shows the Kaspersky Threat Intelligence Portal interface. At the top, there is a navigation bar with options like Home, Reporting, Threat Lookup, WHOIS Tracking, Cloud Sandbox, Data Feeds, and Licensing. Below this is a search bar with the placeholder text 'Hash, IP address, domain, or URL' and a 'Look up' button. A report for the domain 'unspoilportugal.co.uk' is displayed, showing statistics such as 'IPv4 count: 1', 'Files count: -', 'URLs count: ≈ 10 000', and 'Hits count: ≈ 10 000'. The report also includes fields for 'Created', 'Expires', 'Domain', 'Registration organization', and 'Registrar name', all of which are currently empty. A 'Category' field is circled in yellow, containing the text 'APT Related' and a link to 'Gatak - Stealthy Actor Harvesting Data'.

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.

The screenshot shows a report from Kaspersky titled 'Gatak - Stealthy Actor Harvesting Data'. The report is marked as 'TLP: AMBER'. It includes the report ID '20171202' and version '1.0 (8.December.2017)'. The 'Executive summary' section describes Gatak (also known as Stegoloader and GOLD) as an elusive threat actor that engages in data theft through opportunistic watering hole attacks. It mentions that Gatak has thousands of victims worldwide during 2017 and is known to drop old ransomware samples in possible false flag operations, according to Symantec. The report also states that Gatak relies on a chain of payloads during breaches. Below the summary, there are sections for 'Appendix I - Indicators of compromise', 'Stage 0 hashes', and 'Domains and IPs'. The 'Stage 0 hashes' section lists several long alphanumeric strings, and the 'Domains and IPs' section lists 'unspoilportugal.co[.]uk', 'vmx13321.hosting24.com[.]au', and 'ipnc.co[.]kr'.

Портал Kaspersky Threat Intelligence обеспечивает:

- Улучшение и ускорение расследования и реагирования на инциденты. Команды ИБ или SOC получают 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

© АО «Лаборатория Касперского», 2019. Все права защищены.
Зарегистрированные товарные знаки и знаки обслуживания
являются собственностью их правообладателей.

