

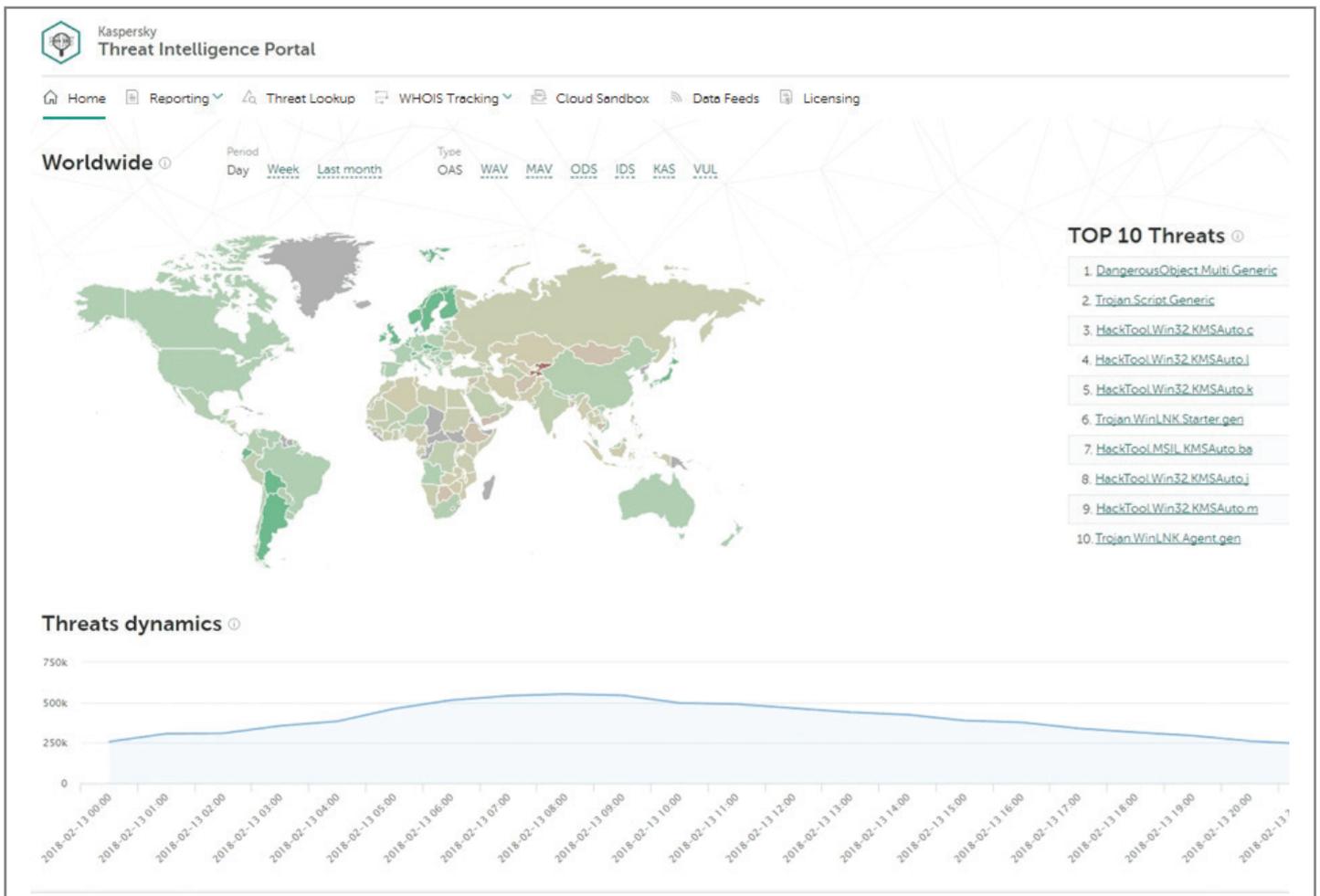
# **The Kaspersky Threat Intelligence Portal: Incident Investigation and Response**

**kaspersky**

<https://www.kaspersky.com/enterprise-security/threat-intelligence>  
[#truecybersecurity](#)

The Kaspersky Threat Intelligence Portal delivers all the knowledge that Kaspersky Lab has collected, refined and categorized over more than twenty years of company history. The platform retrieves the latest detailed threat intelligence about files, URLs, domains, IP addresses, file hashes, threat names, statistical/behavior data, WHOIS/DNS data, etc., allowing incident responders to:

- Determine whether an event in the queue requires an immediate response or additional examination
- Use the first detection as a starting point to ascertain the full scope of an incident – and to respond accordingly
- Define who was affected, what was affected and what the impact was – and provide meaningful information to other relevant departments
- Understand the tactics and techniques used by cybercriminals, as well as their goals, to determine the most effective response



The Threat Intelligence Portal main page has numerous tabs, but for the purpose of this example, let's imagine that we have live evidence. The incident response team obtained a suspicious file sample that initiated communication from inside the network perimeter with an external IP address, outside of normal working hours. So we can go straight to the Cloud Sandbox tab in the top menu.

The Sandbox runs a suspicious object in a virtual machine (VM) with a full-featured OS. It detects an object's malicious activity by analyzing its behavior. VMs are isolated from the real business infrastructure, so detonation won't cause real damage. Just upload your file, select the environment (Windows 7, in this case), select the time (let's try 100 seconds) and start the execution:

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	<p><b>3e5a92eafd63a5d09d986f89a9fd5657</b></p> <p>MD5 3e5a92eafd63a5d09d986f89a9fd5657 Execution environment Windows 7 x64</p> <p>File size 829.41 KB (849 316 B) Execution time 100 sec</p> <p>Analyzed Jun 14, 2018 12:12 Action Execute</p> <p><a href="#">View details</a> <a href="#">Export all results</a></p>
Malware	Jun 14, 2018 12:00	Completed	<p><b>3e5a92eafd63a5d09d986f89a9fd5657</b></p> <p>MD5 3e5a92eafd63a5d09d986f89a9fd5657 Execution environment Windows 7 x64</p> <p>File size 829.41 KB (849 316 B) Execution time 120 sec</p> <p>Analyzed Jun 14, 2018 12:04 Action Execute</p> <p><a href="#">View details</a> <a href="#">Export all results</a></p>

Sandboxes are effective against malware that evades static analysis – that’s why your antivirus could completely miss a suspicious file. Even if this file was identified as “bad,” most antivirus systems won’t explain how bad it is, or what’s actually going on. To gain more details let’s see what happens in the Kaspersky Cloud Sandbox after detonation:

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](#)

**6**  
Detects

- Malware (6)
- Adware and other (0)

**12**  
Suspicious activities

- High (0)
- Medium (0)
- Low (12)

**17**  
Extracted files

- Malicious (3)
- Adware and other (0)
- Clean (4)
- Not categorized (10)

**0**  
Network activities

- 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	735570e1f0cae68b6bb64213aa313c3ba301102f6
Database update	Jun 14, 2018 12:00	File extension	-			SHA-256	b82b3d9019b3e58d17d53453b8a354a25a751b370fe0088e14b31c1...

Results System activities Extracted files Network activities

Running the tested object, a sandbox collects artifacts, analyzes them, and delivers its verdict. Here's the summary: detections (6), suspicious activities (12), extracted files (17), and network activities (0). It's not just a "bad" file; it does a lot of bad things, and they are all listed.

Results   System activities   Extracted files   Network activities

### Sandbox detection names ⓘ [Download data](#)

Zone	Name
High	<a href="#">Trojan.Win32.Pincav.bqeyx</a>
High	<a href="#">HEUR:Trojan.Win32.Generic</a>
High	<a href="#">Trojan.Win32.Gatak.sb</a>
High	<a href="#">Trojan.Win32.Xpun.sb</a>
High	<a href="#">Trojan.Win32.Inject</a>
High	<a href="#">Trojan.Win32.Yakes</a>

### Triggered network rules ⓘ

No data found

### Execution map ⓘ

- 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 ⓘ (20) [Download all](#)

In the Results tab, an incident responder can see screenshots taken during execution. In some cases, the malware tries to evade automatic analysis by waiting for user interaction (entering a password, scrolling through a document, moving the mouse, etc.). The Kaspersky Cloud Sandbox knows many evasion techniques and uses human-simulating technologies to counter them. Screenshots could be helpful too: A researcher can see what's happening in the "test tube" from a human point of view.

Let's switch to the Extracted files tab to see what objects were downloaded, extracted, or dropped. In this case, a malicious file was dropped:

Results		System activities		Extracted files		Network activities	
<b>Downloaded files</b> ⓘ						No data found	
<b>Dropped files</b> ⓘ						<a href="#">Download data</a>	
Zone	MD5	APT ⓘ	Detection name	File name			
Malware	<a href="#">3E5A92EAFD63A5D09D986F89A9FD5657</a>	—	<a href="#">Trojan.Win32.Pincav.bqeyx</a>	3e5a92eafd63a5d09d986f89a9fd5657.exe			
Malware	<a href="#">84C212A2E281C8F2EC7783751FC65265</a>	—	—	3086.exe			
Malware	<a href="#">DE721AE292DD1EB94F1DA2A2538AAAB2</a>	—	<a href="#">HEUR.Trojan.Win32.Generic</a>	9939.exe			

Classic sandbox capabilities would end at this point: you ran the file and you got the list of malicious activities — and that's all. But with the Kaspersky Threat Intelligence Portal, you can jump straight to the Threat Lookup to reveal more detailed intelligence on indicators of compromise and their relationships.

The Threat Lookup is our search engine for security. It contains about 5 petabytes of threat intelligence, collected and categorized by Kaspersky Lab over the past 20 years: file hashes, statistical/behavior data, WHOIS/DNS data, URLs, IP addresses, and so forth.

So, after we run our sample in the sandbox, we instantly use sandbox results as search queries for the Threat Lookup — just by clicking on the object (an MD5 hash in this case)



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 <a href="#">Trojan.Win32.Yakes</a>	Jun 05, 2015 08:44 <a href="#">Trojan.Win32.Yakes.kubx</a>
--	---

### File signatures and certificates

No data found

Now we have a more detailed report on the malware. Let's scroll through the Threat Lookup results to see which URLs were accessed by the malware we're exploring:

### File accessed following URLs

[Download data](#)

Status	URL
Dangerous	<a href="https://unspoilportugal.co.uk/report_N_0027_">unspoilportugal.co.uk/report_N_0027_</a>
Dangerous	<a href="https://unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000">unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000</a>

Here's a URL marked as "Dangerous." Again, let's drill down to that malicious URL to see what our Threat Lookup has on it:

The screenshot shows the Kaspersky Threat Intelligence Portal interface. At the top, there's a navigation bar with '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. The search results show a report for the domain 'unspoilportugal.co.uk' with a status of 'Dangerous'. A table of statistics is visible, including IPv4 count (1), Files count (—), URLs count (≈ 10 000), and Hits count (≈ 10 000). The report details show 'Registration organization: None' and 'Registrar name: None'. The 'Category' field is circled in yellow and contains the text 'APT Related' and 'Gatak - Stealthy Actor Harvest...'. There are also links for 'Copy request' and 'Export all results'.

It turns out that the malicious URL in question relates to an APT attack! The Kaspersky Threat Intelligence Portal offers to download an APT report. This PDF includes an executive summary, deep technical details, and a list of related indicators of compromise. It's worth checking to find out if anything similar has happened to your organization and to timely develop specific use cases for the detection of the described attack.

The PDF report header features the Kaspersky logo on the right and 'TLP: AMBER' on the left. The main title is 'Gatak - Stealthy Actor Harvesting Data'. Below the title, it lists 'Report Id: 20171202' and 'Version: 1.0 (8.December.2017)'. The section 'Executive summary' begins with a paragraph: '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.' The text ends with 'During breaches, Gatak relies on a chain of payloads which correspond to several stages of attack. The'.

This section of the PDF report is titled 'Appendix I - Indicators of compromise' and 'Stage 0 hashes'. It lists three SHA-256 hashes: '0AE26BA127904EC354F228B316F044A1', '0B20B941D2B9372D875410FFEB53C473', and '166200FE58CE0EABE40B22BE200DE4734'.

This section of the PDF report is titled 'Domains and IPs'. It lists three domains: 'unspoilportugal.co[.]uk', 'vmx13321.hosting24.com[.]au', and 'ipnc.co[.]kr'.

With the Kaspersky Threat Intelligence Portal you can:

- Improve and accelerate your incident response and forensic capabilities by giving security/SOC teams meaningful information about threats, and global insights into what lies behind targeted attacks. Diagnose and analyze security incidents on hosts and the network more efficiently and effectively, and prioritize signals from internal systems against unknown threats, minimizing incident response time and disrupting the kill chain before critical systems and data are compromised.
- Conduct deep searches into threat indicators such as IP addresses, URLs, domains or file hashes, with highly validated threat context that allows you to prioritize attacks, improve staffing and resource allocation decisions, and focus on mitigating the threats that pose the most risk to your business.
- Mitigate targeted attacks. Enhance your security infrastructure with tactical and strategic threat intelligence by adapting defensive strategies to counter the specific threats your organization faces.

---

Cyber Threats News: [www.securelist.com](http://www.securelist.com)  
IT Security News: [business.kaspersky.com/](http://business.kaspersky.com/)

---

[www.kaspersky.com](http://www.kaspersky.com)

**kaspersky** BRING ON  
THE FUTURE