

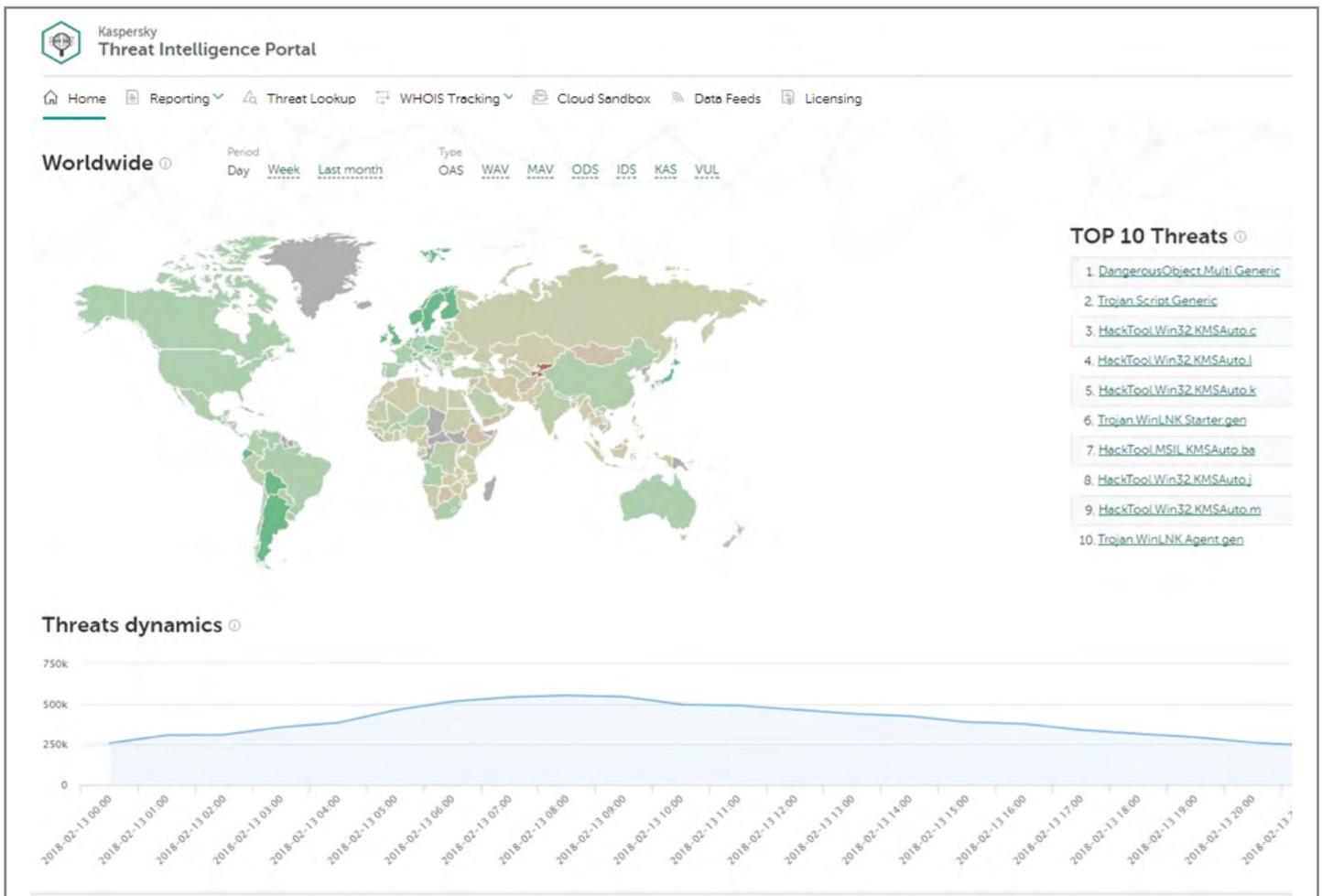
# **Das Kaspersky Threat Intelligence Portal: Vorfallsuntersuchung und -abwehr**

**kaspersky**

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

Das Kaspersky Threat Intelligence Portal bietet Ihnen Zugriff auf das Wissen, das Kaspersky in seinen 20 Jahren Unternehmensgeschichte gewonnen, verfeinert und kategorisiert hat. Die Plattform erfasst die neuesten ausführlichen Bedrohungsinformationen zu Dateien, URLs, Domains, IP-Adressen, Datei-Hashes, Bedrohungsnamen, Statistik-/Verhaltensdaten, WHOIS-/DNS-Daten usw. und bietet Vorfallsreaktionsteams folgende Möglichkeiten:

- Sie können bestimmen, ob ein Ereignis in der Warteschlange eine umgehende Reaktion oder zusätzliche Untersuchung erfordert
- Sie können die erste Erkennung als Ausgangspunkt zur Untersuchung des vollen Umfangs des Vorfalls nutzen und entsprechend reagieren
- Sie können definieren, wer und was betroffen ist und welche Auswirkungen der Vorfall hatte und anderen Abteilungen aussagekräftige Informationen bereitstellen
- Sie erhalten Informationen zu den Taktiken und Techniken der Cyberkriminellen sowie zu ihren Zielen, um die effektivste Reaktion zu ermitteln



Die Hauptseite des Threat Intelligence Portal umfasst verschiedene Registerkarten, dieses Beispiel soll jedoch die Untersuchung eines Livevorfalls veranschaulichen. Das Incident Response Team hat eine verdächtige Dateiprobe erhalten, die außerhalb der Geschäftszeiten vom Netzwerkperimeter aus eine Kommunikation mit einer externen IP-Adresse eingeleitet hat. Wir wechseln also direkt zur Registerkarte „Cloud Sandbox“ im oberen Menü.

Die Sandbox führt das verdächtige Objekt in einer virtuellen Maschine (VM) mit voll funktionsfähigem Betriebssystem aus. Sie erkennt die schädliche Aktivität des Objekts, indem sie sein Verhalten analysiert. VMs sind von der Unternehmensinfrastruktur isoliert, sodass die Ausführung der Malware keinen Schaden anrichten kann. Laden Sie einfach die Datei hoch, wählen Sie die Umgebung aus (in diesem Fall Windows 7), legen Sie einen Zeitraum fest (wir versuchen es mit 100 Sekunden) und starten Sie die Ausführung:



You are using a commercial version of the service

### Cloud Sandbox



3e5a92eafd63a5d09d986f89a9fd5657 829.41 KB

File execution environment

File execution time (sec)

Windows 7 x64

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 sind sehr effektiv bei Malware, die statische Analysen umgeht. Normale Antivirenprogramme würden solche verdächtigen Dateien einfach übersehen. Und selbst wenn die Datei als schädlich eingestuft wird, bieten die meisten Antivirensysteme keine Erklärung dazu, wie schädlich sie ist und warum. So erhalten Sie ausführliche Informationen dazu, was nach der Ausführung in der Kaspersky Cloud Sandbox passiert:



Recent file execution results / Sandbox report

3e5a92eafd63a5d09d986f89a9fd5657 Malware

### Summary



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	735570e1f0cae68bbb64213aa313c3ba301102f6
Database update	Jun 14, 2018 12:00	File extension	-	SHA-256	b82b3d9019b3e58d17d53453b8a354a25a751b370fe0088e14b31c1...		

Wenn das Testobjekt ausgeführt wird, erfasst die Sandbox Artefakte, analysiert sie und stellt das Ergebnis bereit. Im Folgenden finden Sie die Zusammenfassung: Erkennungen (6), verdächtige Aktivitäten (12), extrahierte Dateien (17) und Netzwerkaktivitäten (0). Sie erhalten nicht einfach nur einen Hinweis auf eine „schädliche Datei“: Sie erfahren, welche schädlichen Aktionen die Datei genau ausführt.

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\WmiPrivSE.exe process has obtained the privilege SeDebugPrivilege.
Low	200	The \$windir\system32\wbem\WmiPrivSE.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](#)

Auf der Registerkarte „Ergebnisse“ können Incident Response-Teams Screenshots einsehen, die während der Ausführung erstellt wurden. In manchen Fällen versucht die Malware, die automatische Analyse zu umgehen, indem sie auf eine Benutzerinteraktion, wie z.B. die Eingabe eines Passworts, das Scrollen in einem Dokument, das Bewegen des Mauszeigers usw., wartet. Die Kaspersky Cloud Sandbox kennt zahlreiche Umgehungstaktiken und simuliert menschliche Interaktion, um sie zu verhindern. Mithilfe von Screenshots können Analysten ermitteln, was aus menschlicher Sicht bei Tests passiert.

Wechseln wir jetzt zur Registerkarte „Extrahierte Dateien“. Hier wird angezeigt, welche Objekte heruntergeladen, extrahiert oder abgelegt wurden. In diesem Fall wurde eine schädliche Datei abgelegt:

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

Herkömmliche Sandbox-Funktionen wären beendet, nachdem Sie die Datei ausgeführt und eine Liste schädlicher Aktivitäten erhalten haben. Doch mit dem Kaspersky Threat Intelligence Portal können Sie direkt zu Kaspersky Threat Lookup wechseln, um ausführliche Informationen zu den Gefährdungsindikatoren und ihren Beziehungen anzuzeigen.

Threat Lookup ist unsere Suchmaschine für Sicherheit. Sie enthält ca. fünf Petabyte an Bedrohungsinformationen, die Kaspersky Lab in den letzten 20 Jahren erfasst und kategorisiert hat: Datei-Hashes, Statistik-/Verhaltensdaten, WHOIS-/DNS-Daten, URLs, IP-Adressen usw.

Nachdem unsere Probe nun also die Sandbox durchlaufen hat, verwenden wir die Ergebnisse umgehend als Suchanfragen für Threat Lookup, indem wir einfach auf das Objekt klicken (in diesem Fall ein MD5-Hash)



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

So erhalten wir ausführlichere Informationen zur untersuchten Malware. Scrollen wir nun durch die Threat Lookup-Ergebnisse, um herauszufinden, auf welche URLs die Malware zugegriffen hat:

### 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>

Hier ist beispielsweise eine URL, die als „gefährlich“ markiert ist. Auch diese schädliche URL suchen wir in Threat Lookup, um zu sehen, welche Informationen hierzu verfügbar sind:

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 'Enter your request here' and a 'Look up' button. The search results are displayed in a table format. The first row shows the domain 'unspoilportugal.co.uk' with a 'Report for Domain: Dangerous' status. The table includes various statistics such as IPv4 count (1), Files count, URLs count (≈ 10 000), and Hits count (≈ 10 000). It also lists registration details like 'Registration organization: None' and 'Registrar name: None'. A yellow circle highlights the 'Category' field, which is 'APT Related' and includes a link to 'Gatak - Stealthy Actor Harvesting Data'.

Das Ergebnis zeigt, dass die fragliche URL zu einem APT-Angriff gehört. Über das Kaspersky Threat Intelligence Portal können Sie einen entsprechenden APT-Bericht herunterladen. Diese PDF beinhaltet eine Zusammenfassung, eingehende technische Details sowie eine Liste zugehöriger Gefährdungsindikatoren. Analysten können mit diesem Bericht überprüfen, ob in Ihrem Unternehmen schon einmal etwas Ähnliches passiert ist, und rechtzeitig Anwendungsfälle zur Erkennung des entsprechenden Angriffs entwickeln.

The cover page of the report features the Kaspersky logo at the top right. On the left, it indicates 'TLP: AMBER'. The main title is 'Gatak - Stealthy Actor Harvesting Data' in a large, bold font. Below the title, the report ID '20171202' and version '1.0 (8.December.2017)' are listed. The section 'Executive summary' is highlighted in blue. The summary text describes Gatak as an elusive threat actor engaged in data theft through opportunistic watering hole attacks, mentioning its discovery in 2017 and its ability to harvest data and drop ransomware samples. A large 'TLP' watermark is visible in the background.

This section is titled 'Appendix I - Indicators of compromise' and focuses on 'Stage 0 hashes'. It lists three SHA-256 hashes: 0AE26BA127904EC354F228B316F044A1, 0B20B941D2B9372D875410FFEB53C473, and 166200FE58CF0EABE40B33BE300DE4734. A large 'TLP' watermark is visible in the background.

This section is titled 'Domains and IPs' and lists three domains: unspoilportugal.co[.]uk, vmx13321.hosting24.com[.]au, and ipnc.co[.]kr. A large 'TLP' watermark is visible in the background.

Das Kaspersky Threat Intelligence Portal bietet folgende Vorteile:

- Verbessern und beschleunigen Sie Ihre Vorfallsreaktion und forensischen Funktionen, indem Sie Ihren Sicherheits-/SOC-Teams Zugriff auf relevante Bedrohungsinformationen sowie globale Erkenntnisse über die Hintergründe von gezielten Angriffen bereitstellen. Diagnostizieren und analysieren Sie Sicherheitsvorfälle auf Hosts und im Netzwerk effizienter und wirkungsvoller. Priorisieren Sie Signale von internen Systemen gegenüber unbekanntem Bedrohungen, verkürzen Sie so die Vorfallsreaktionszeit und unterbrechen Sie die Kill Chain, bevor entscheidende Systeme und Daten in Mitleidenschaft gezogen werden.
- Führen Sie anhand hochzuverlässiger Bedrohungskontexte detaillierte Suchen innerhalb der Bedrohungsindikatoren aus, z. B. in IP-Adressen, URLs, Domänen oder Datei-Hashes, um Angriffe zu priorisieren, Entscheidungen über Personal- und Ressourcenzuteilungen zu verbessern und sich auf die Abwehr derjenigen Bedrohungen zu konzentrieren, die das größte Risiko für Ihr Unternehmen darstellen.
- Wehren Sie gezielte Angriffe ab. Verstärken Sie Ihre Sicherheitsinfrastruktur durch taktische und strategische Bedrohungsinformationen, indem Sie Verteidigungsstrategien an die spezifischen Bedrohungen anpassen, mit denen Ihr Unternehmen konfrontiert ist.

---

Cyber Threat News: <https://de.securelist.com/>  
IT Security News: [www.kaspersky.de/blog/b2b/](http://www.kaspersky.de/blog/b2b/)

---

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

**kaspersky** BRING ON  
THE FUTURE