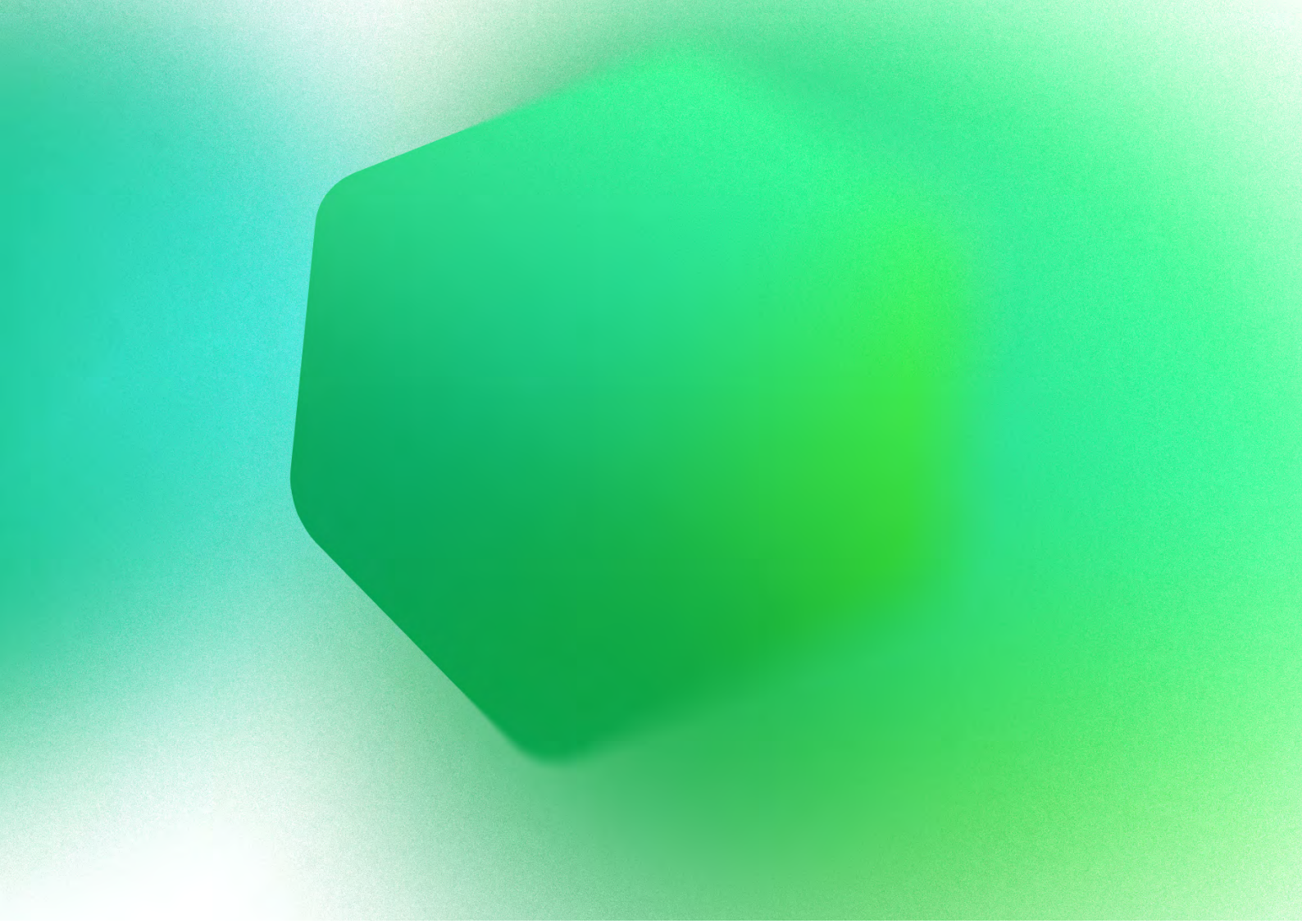


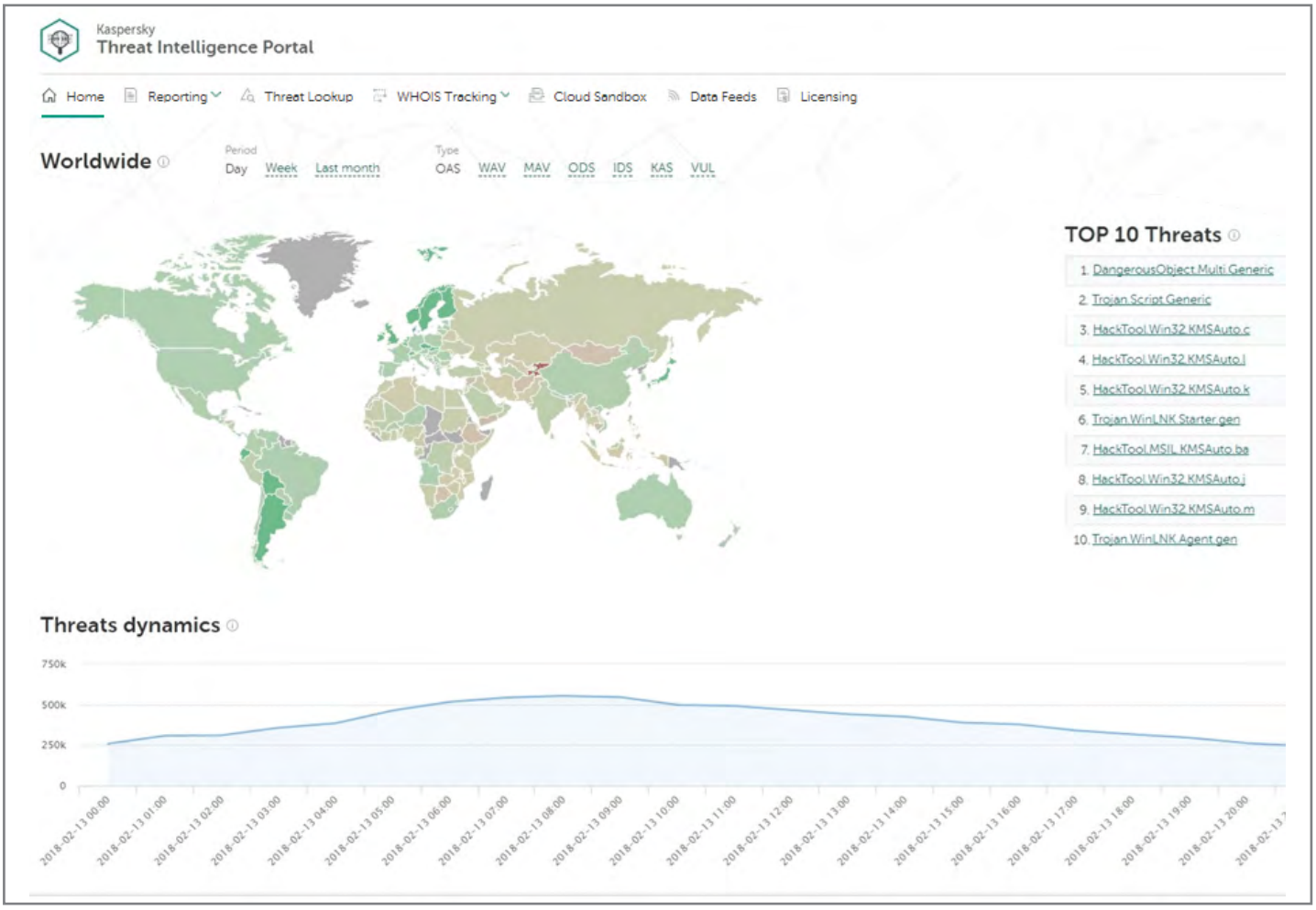
Das Kaspersky Threat Intelligence Portal: Vorfallsuntersuchung und -abwehr

kaspersky

https://www.kaspersky.de/enterprise-security/threat-intelligence
#truecybersecurity

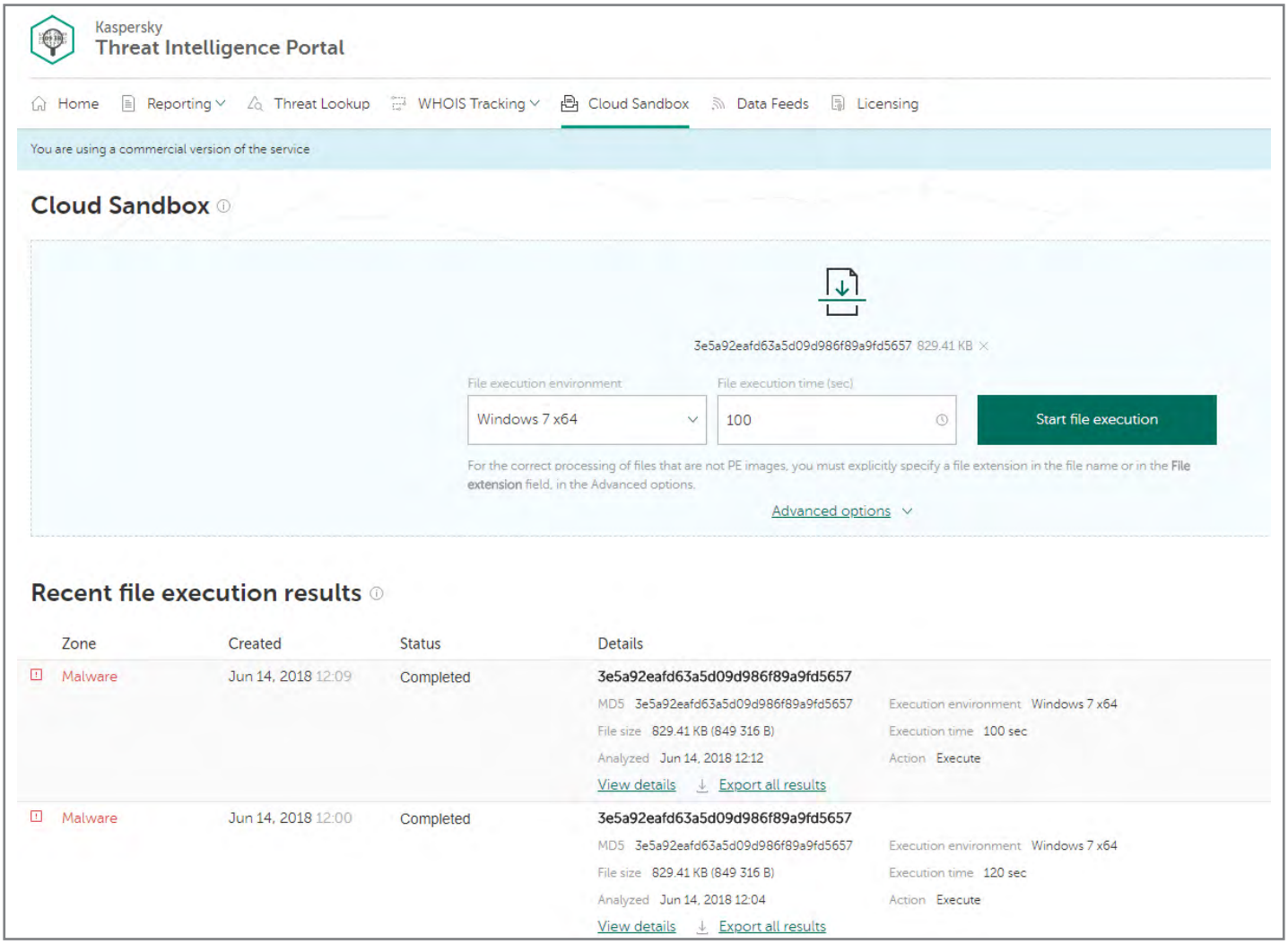
Das Kaspersky Threat Intelligence Portal bietet Ihnen Zugriff auf das Wissen, das Kaspersky in seinen 20 Jahren Unternehmensgeschichte gewonnen, verfeinert und kategorisiert hat. Die Plattform erfasst die neuesten ausführlichen Bedrohungsinformationen zu Dateien, URLs, Domains, IP-Adressen, Datei-Hashes, 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

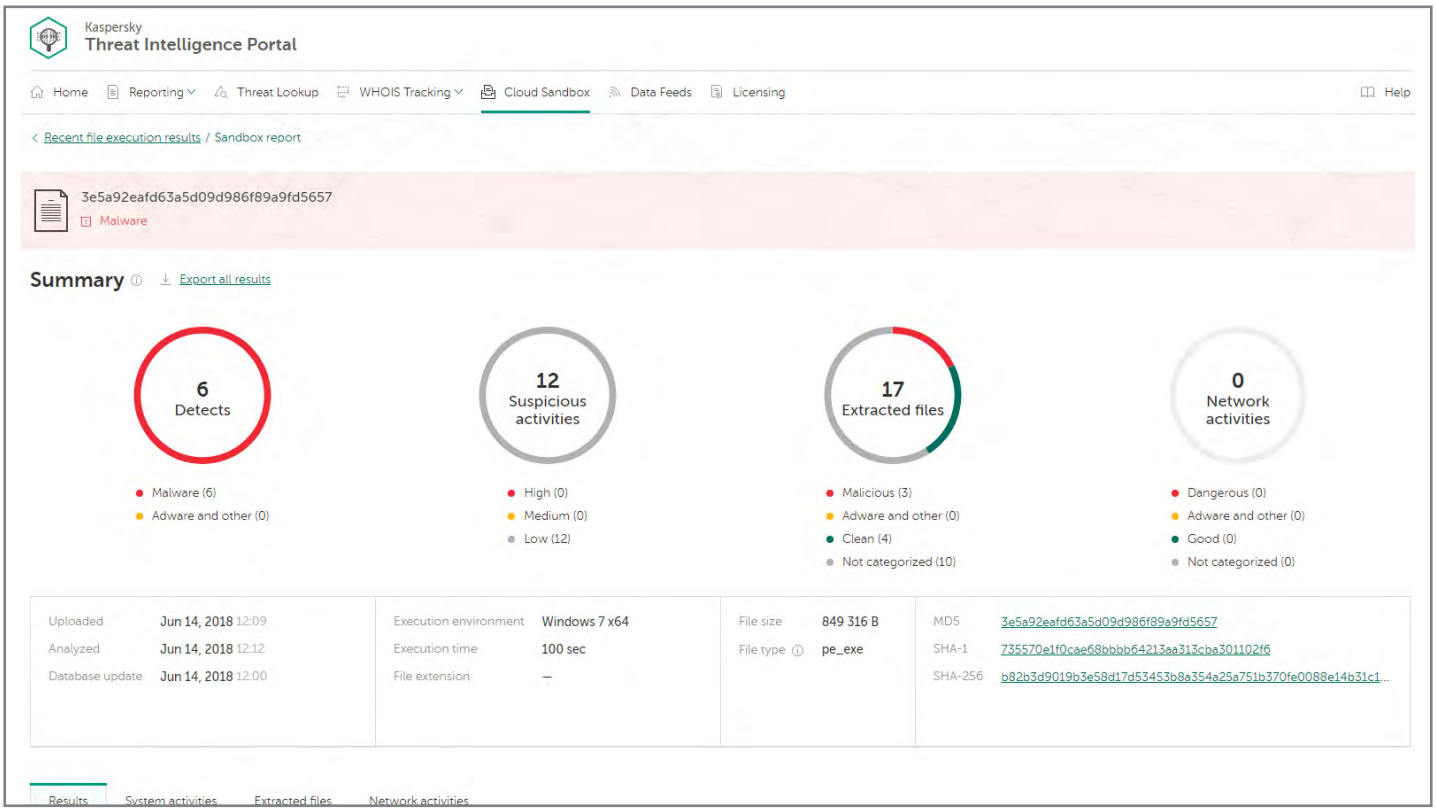


Die Hauptseite des Threat Intelligence Portal umfasst verschiedene Registerkarten, dieses Beispiel soll jedoch die Untersuchung eines Livevorfalls veranschaulichen. Das Incident Response Team hat eine verdächtige Dateiprobe erhalten, die außerhalb der Geschäftszeiten vom Netzwerkperimeter aus eine Kommunikation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

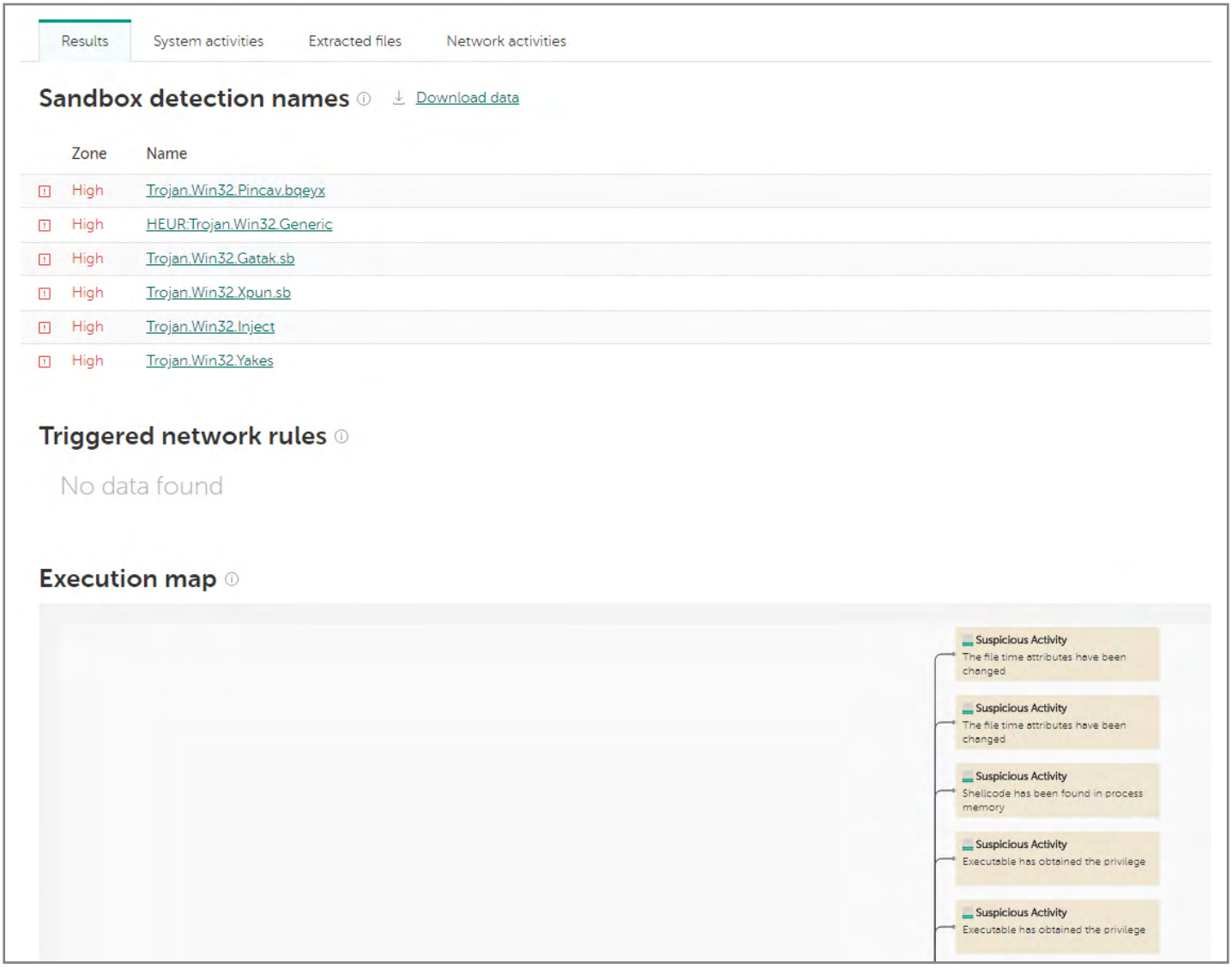
Die Sandbox führt das verdächtige Objekt in einer virtuellen Maschine (VM) mit voll funktionsfähigem Betriebssystem aus. Sie erkennt die schädliche Aktivität des Objekts, indem sie sein Verhalten analysiert. VMs sind von der Unternehmensinfrastruktur isoliert, sodass die Ausführung der Malware keinen 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:

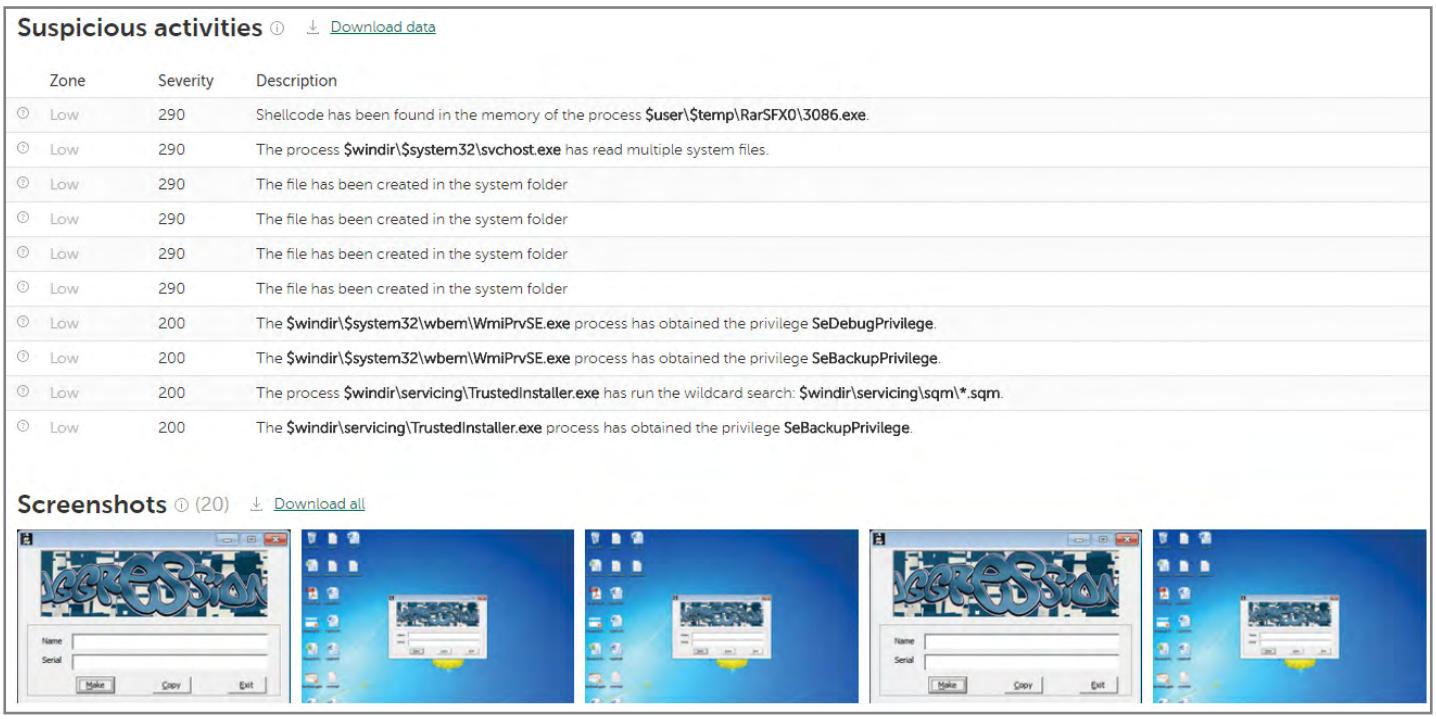


Sandboxes sind sehr effektiv bei Malware, die statische Analysen umgeht. Normale Antivirenprogramme würden solche verdächtigen Dateien einfach übersehen. Und selbst wenn die Datei als schädlich eingestuft wird, bieten die meisten Antivirensysteme keine Erklärung dazu, wie schädlich sie ist und warum.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



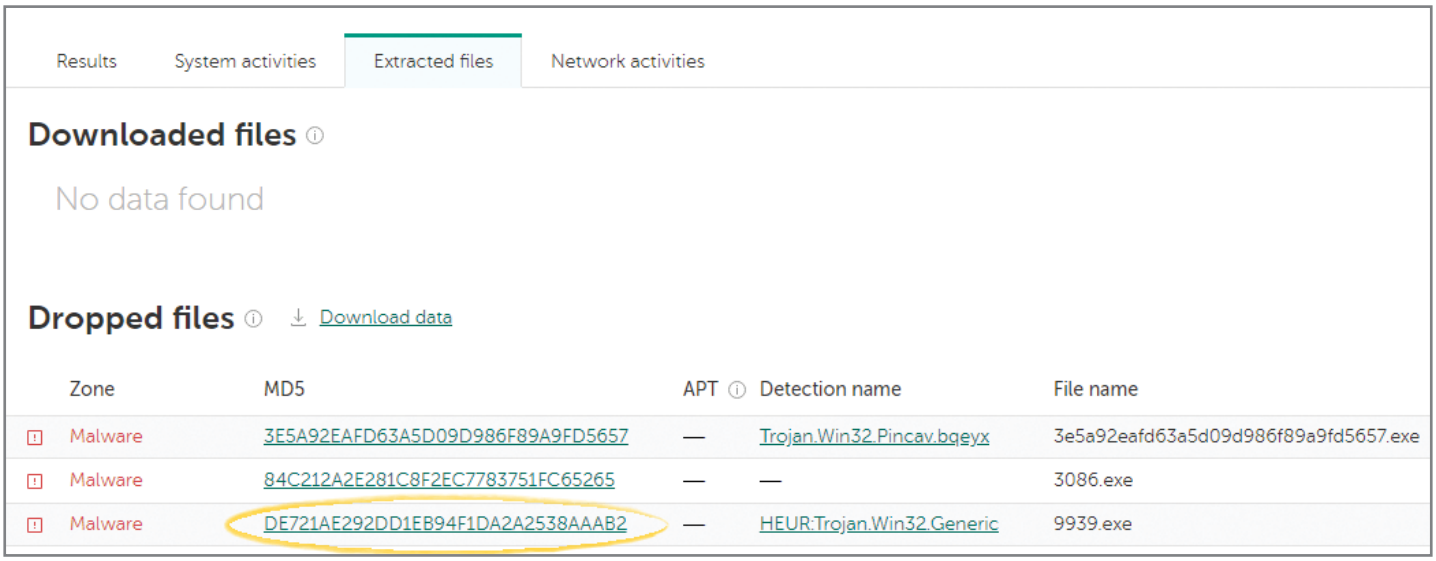
Wenn das Testobjekt ausgeführt wird, erfasst die Sandbox Artefakte, analysiert sie und stellt das Ergebnis bereit. Im Folgenden finden Sie die Zusammenfassung: Erkennungen (6), verdächtige Aktivitäten (12), extrahierte Dateien (17) und Netzwerkaktivitäten (0). Sie erhalten nicht einfach nur einen Hinweis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





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.

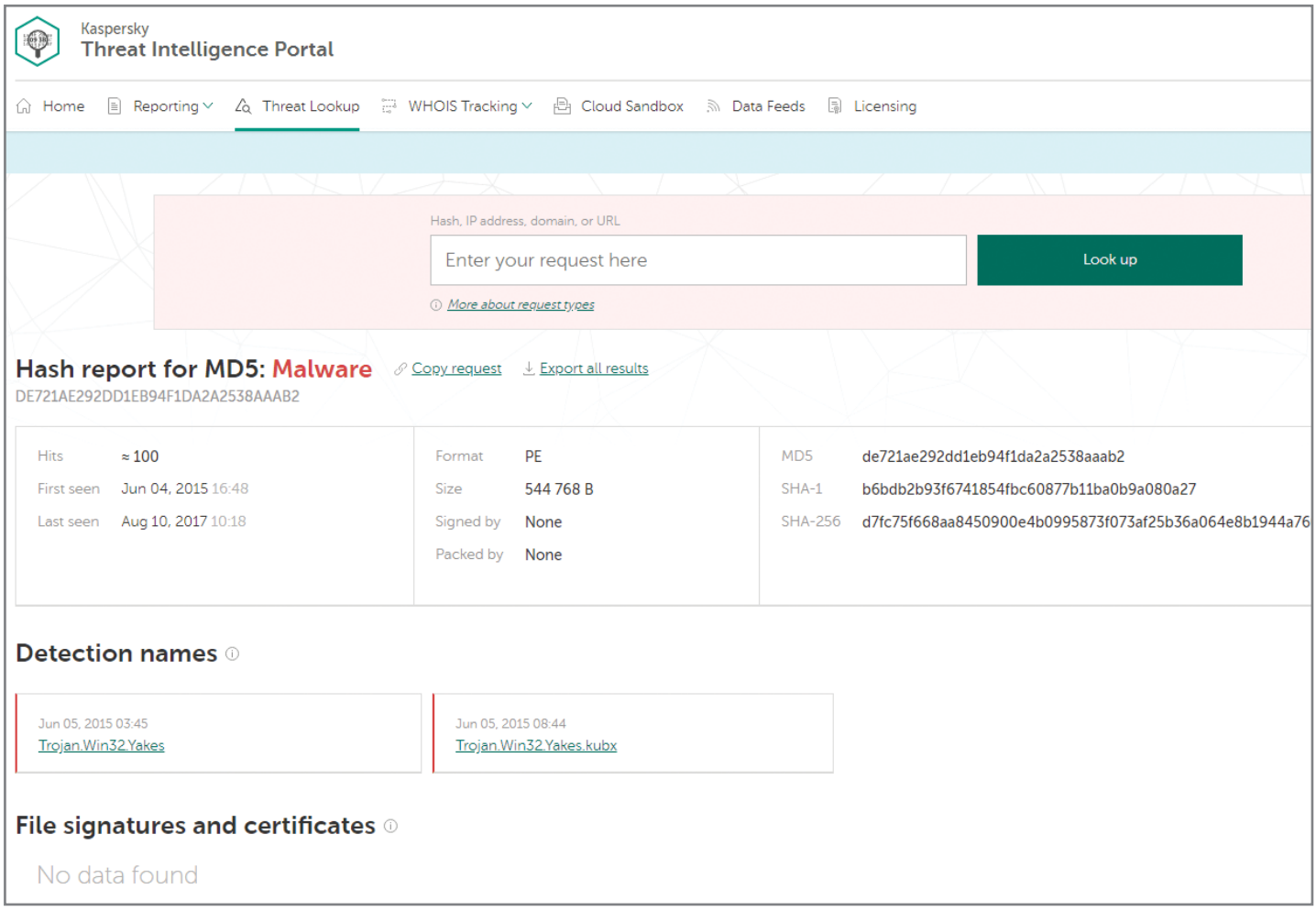
Wechseln wir jetzt zur Registerkarte „Extrahierte Dateien“. Hier wird angezeigt, welche Objekte heruntergeladen, extrahiert oder abgelegt wurden. In diesem Fall wurde eine schädliche Datei abgelegt:



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 report for MD5: Malware

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

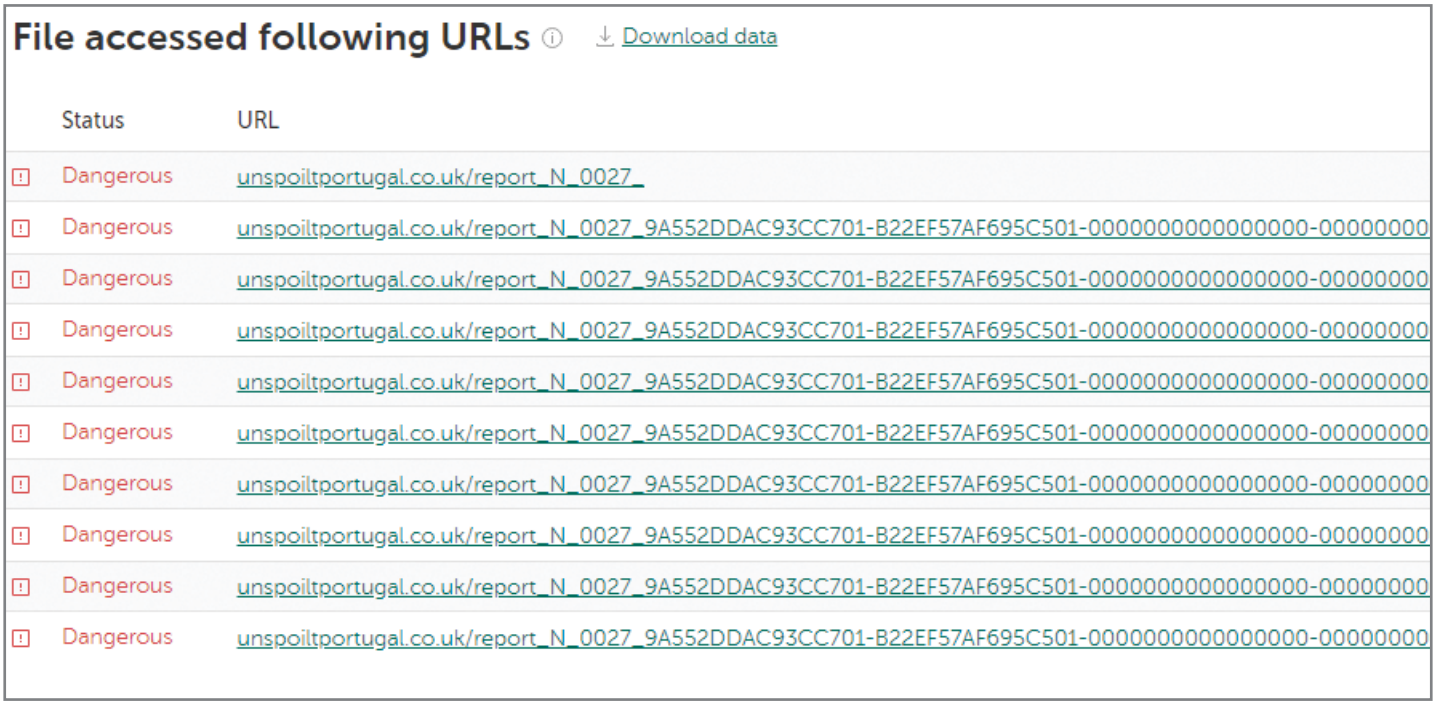
Jun 05, 2015 03:45
Trojan.Win32.Yakes

Jun 05, 2015 08:44
Trojan.Win32.Yakes.kubx

File signatures and certificates

No data found

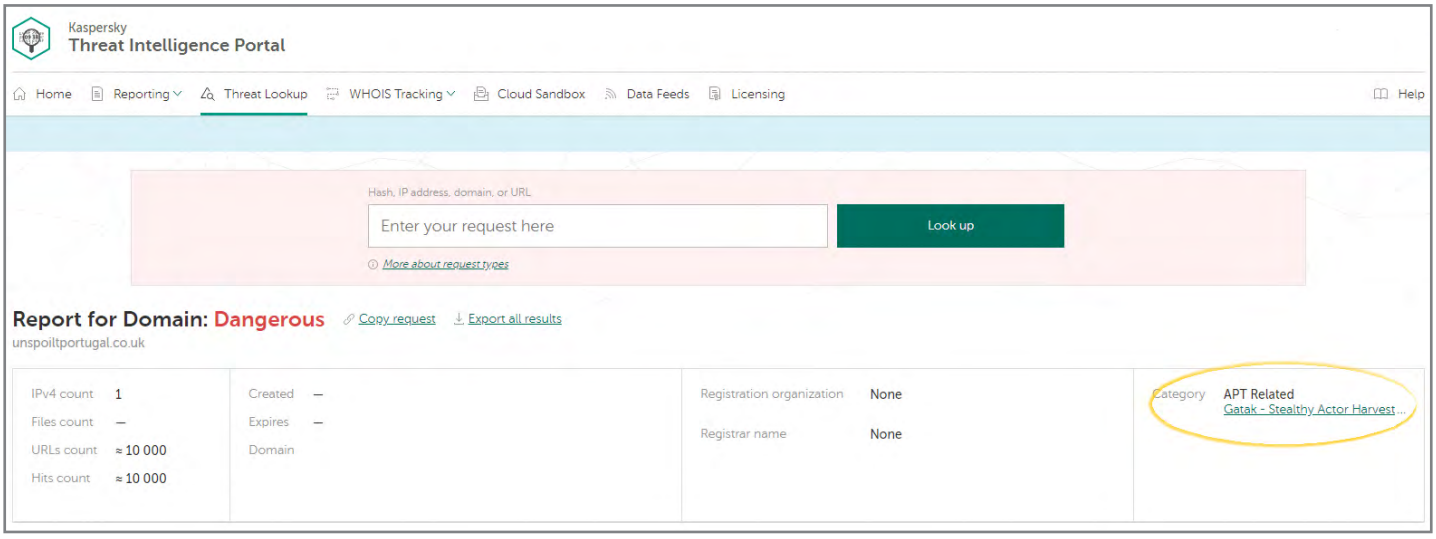
So erhalten wir ausführlichere Informationen zur untersuchten Malware. Scrollen wir nun durch die Threat Lookup-Ergebnisse, um herauszufinden, auf welche URLs die Malware zugegriffen hat:



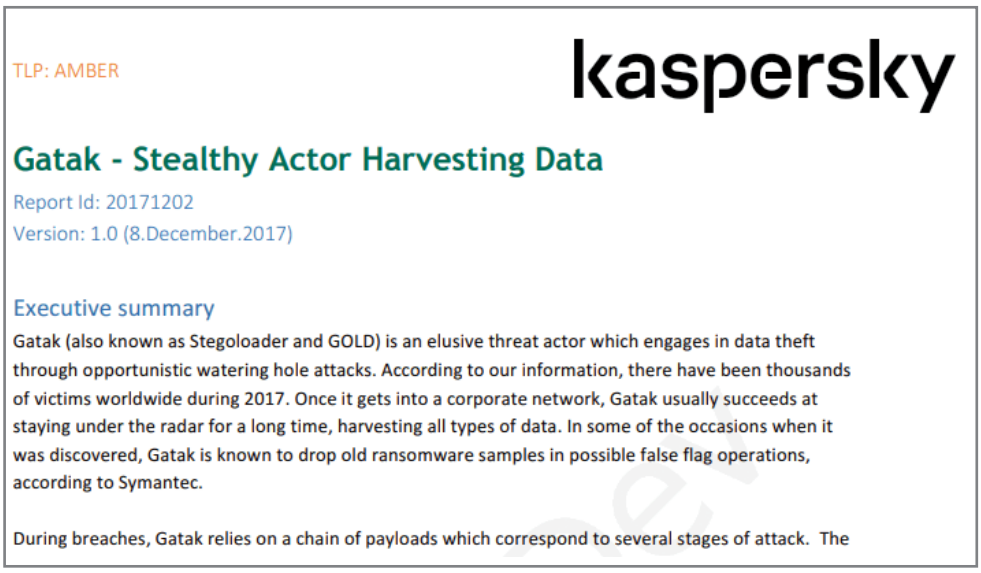
File accessed following URLs

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

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:



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.


TLP: AMBER

kaspersky

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.

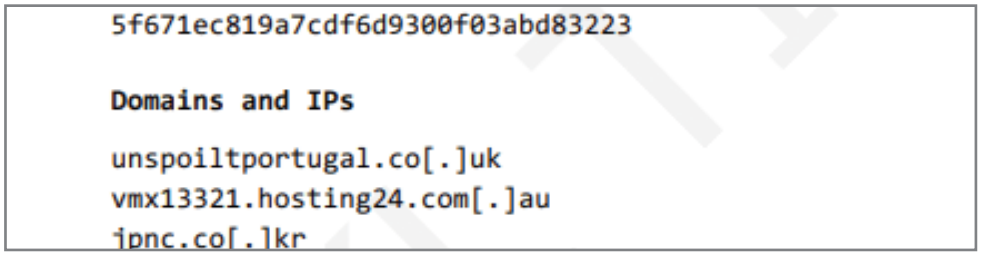
During breaches, Gatak relies on a chain of payloads which correspond to several stages of attack. The


Appendix I - Indicators of compromise

Stage 0 hashes

0AE26BA127904EC354F228B316F044A1

0B20B941D2B9372D875410FFEB53C473


5f671ec819a7cdf6d9300f03abd83223

Domains and IPs

unspoiltportugal.co[.]uk

vmx13321.hosting24.com[.]au

jpnc.co[.]kr

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 unbekannten 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/

www.kaspersky.de

kaspersky BRING ON THE FUTURE