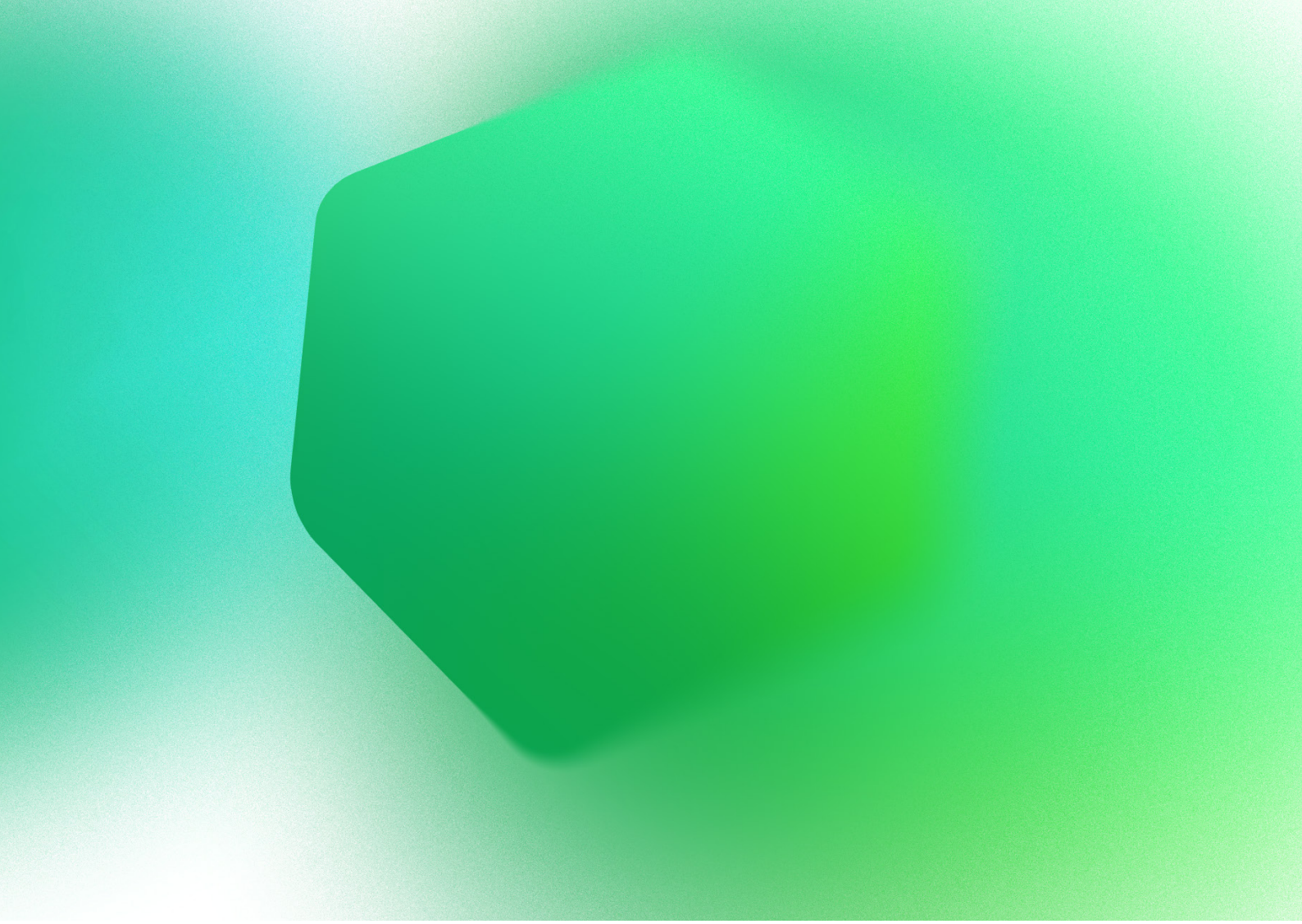


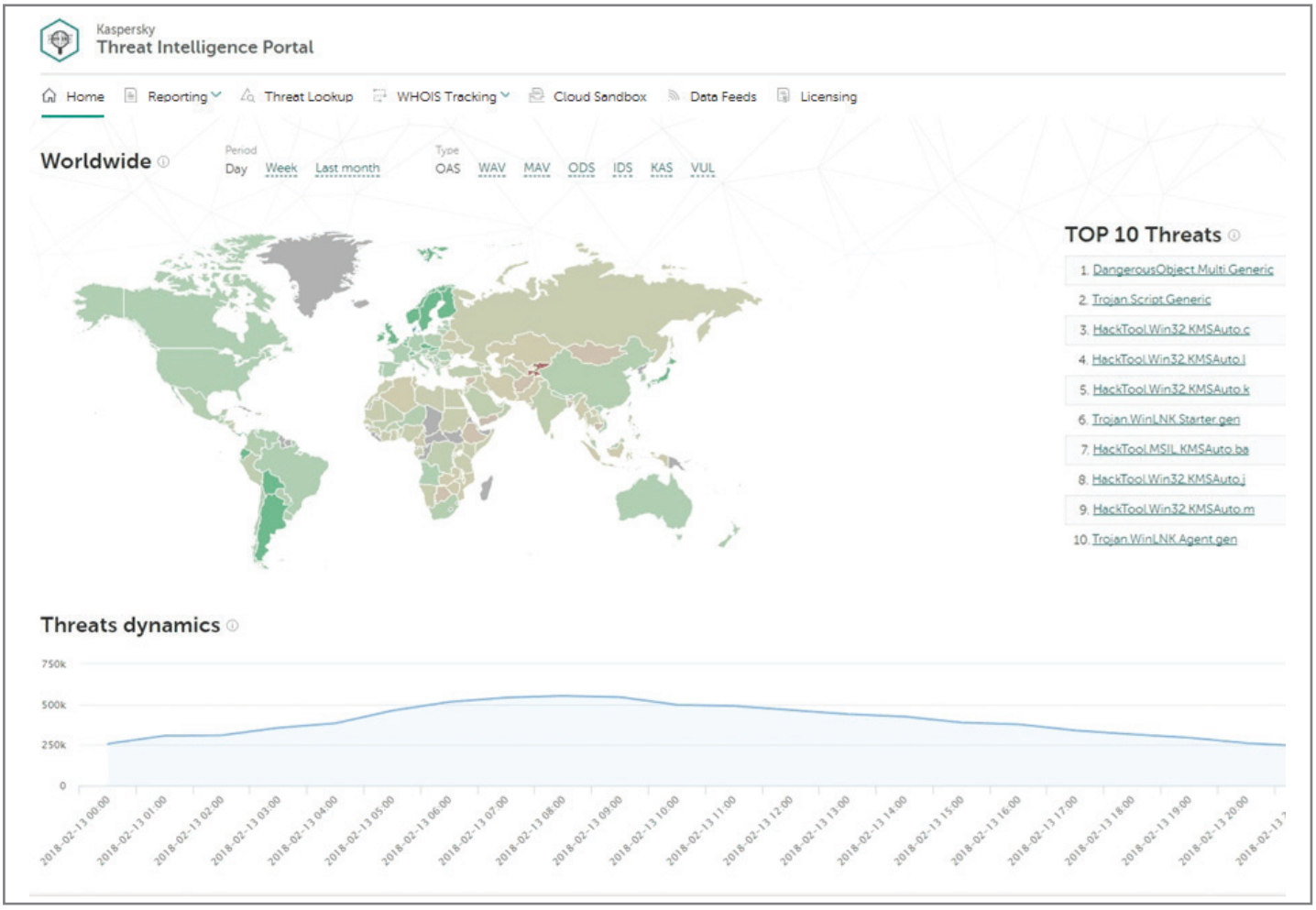
The Kaspersky Threat Intelligence Portal: Incident Investigation and Response

kaspersky

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

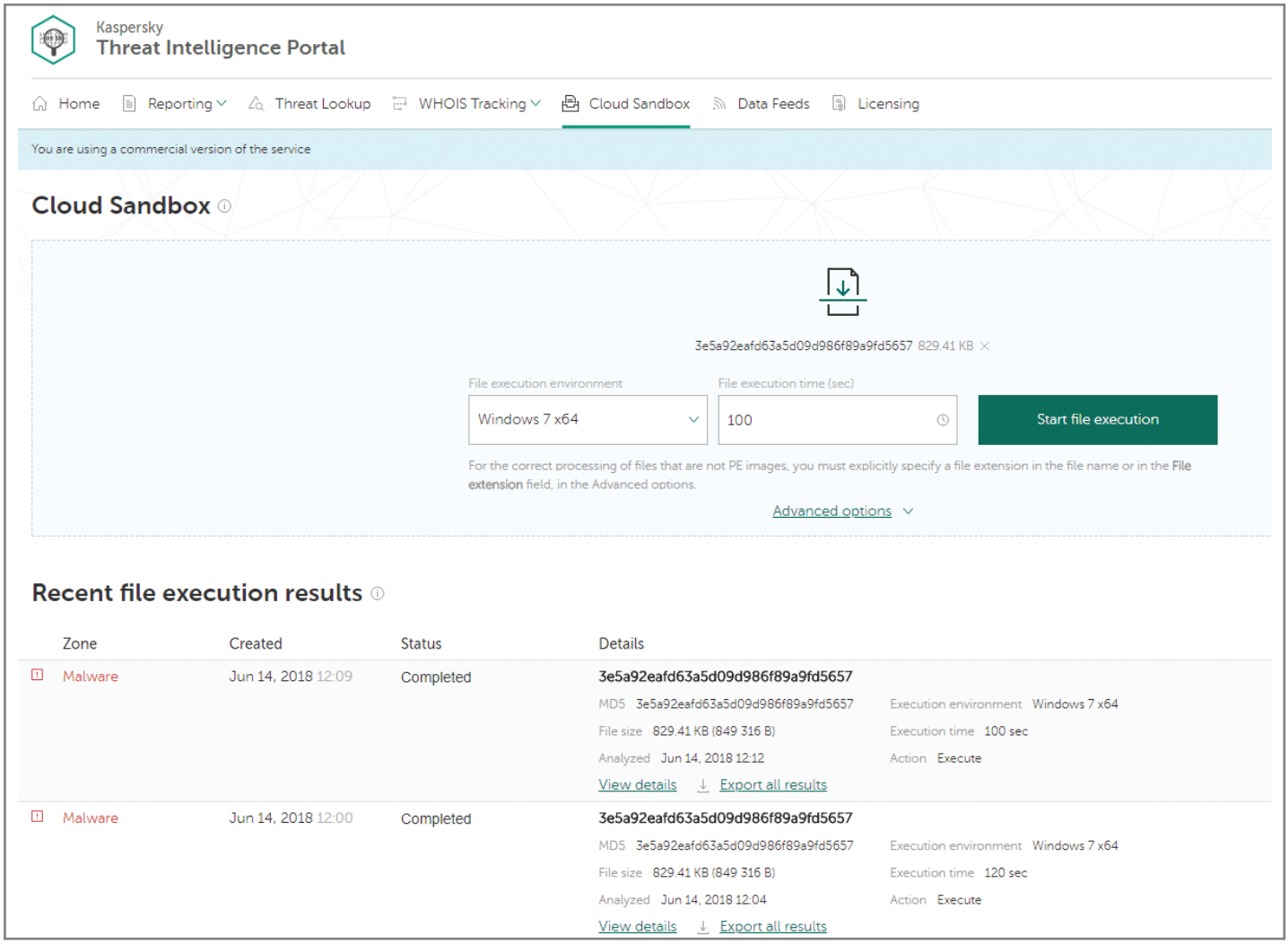
The Kaspersky Threat Intelligence Portal delivers all the knowledge that Kaspersky Lab has collected, refined and categorized over more than twenty years of company history. The platform retrieves the latest detailed threat intelligence about files, URLs, domains, IP addresses, file hashes, threat names, 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

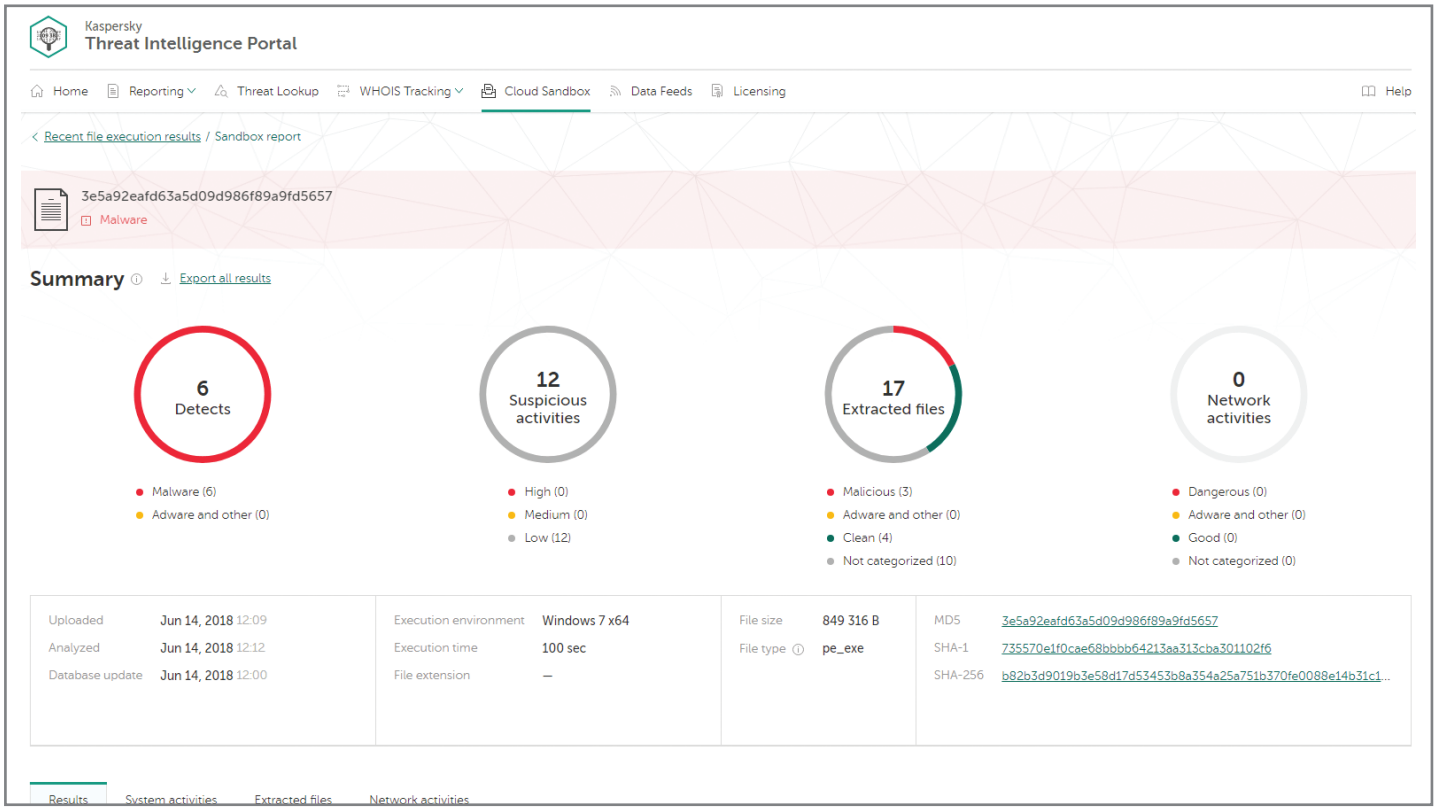


The Threat Intelligence Portal main page has numerous tabs, but for the purpose of this example, let's imagine that we have live evidence. The incident response team obtained a suspicious file sample that initiated communication from inside the network perimeter with an external IP address, outside of 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:



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:



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

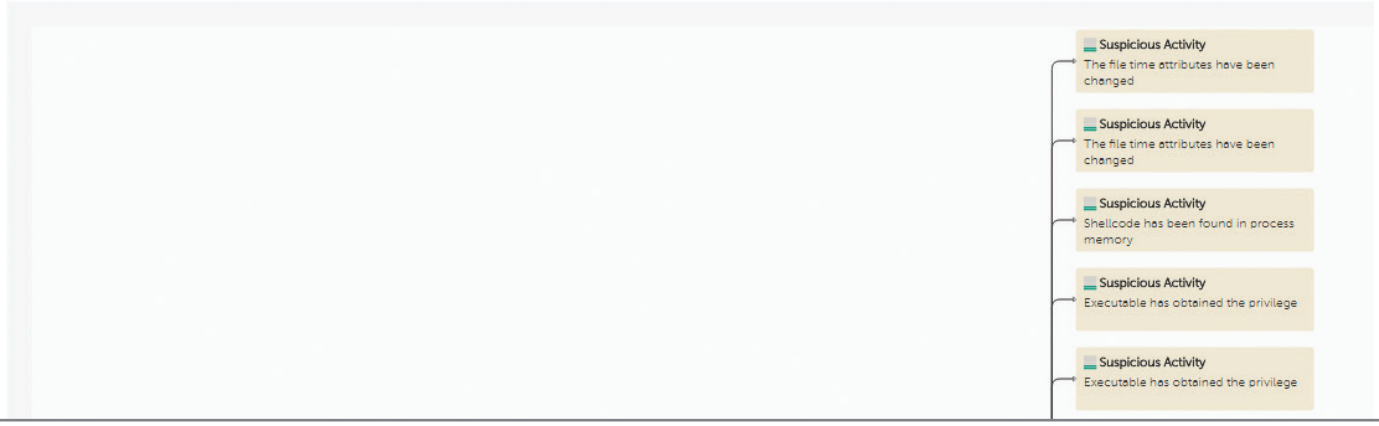
Download data

Zone	Name
High	Trojan.Win32.Pincav.bqeyx
High	HEUR:Trojan.Win32.Generic
High	Trojan.Win32.Gatak.sb
High	Trojan.Win32.Xpun.sb
High	Trojan.Win32.Inject
High	Trojan.Win32.Yakes

Triggered network rules

No data found

Execution map



Suspicious activities

Download data

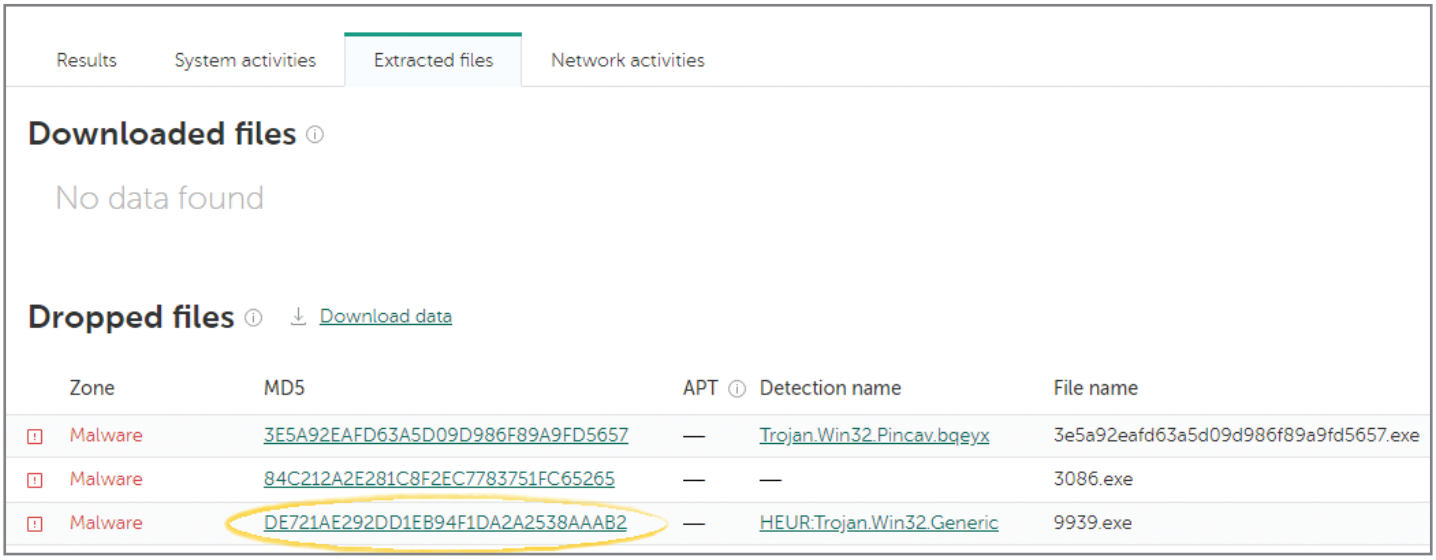
Zone	Severity	Description
Low	290	Shellcode has been found in the memory of the process **$user\$temp\RarSFX0\3086.exe**.
Low	290	The process **$windir\$system32\svchost.exe** has read multiple system files.
Low	290	The file has been created in the system folder
Low	290	The file has been created in the 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.

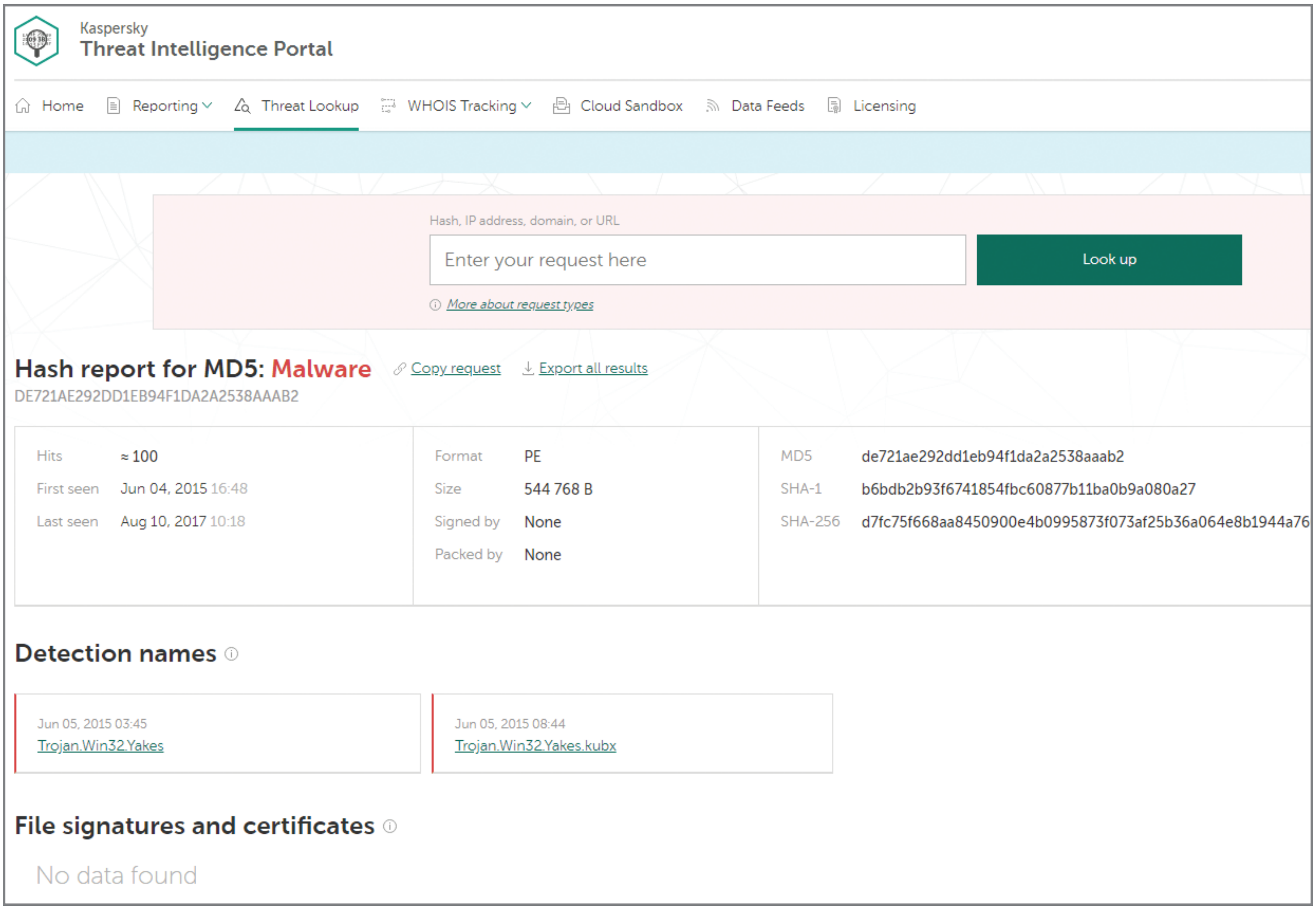
Let's switch to the Extracted files tab to see what objects were downloaded, extracted, or dropped. In this case, a malicious file was dropped:



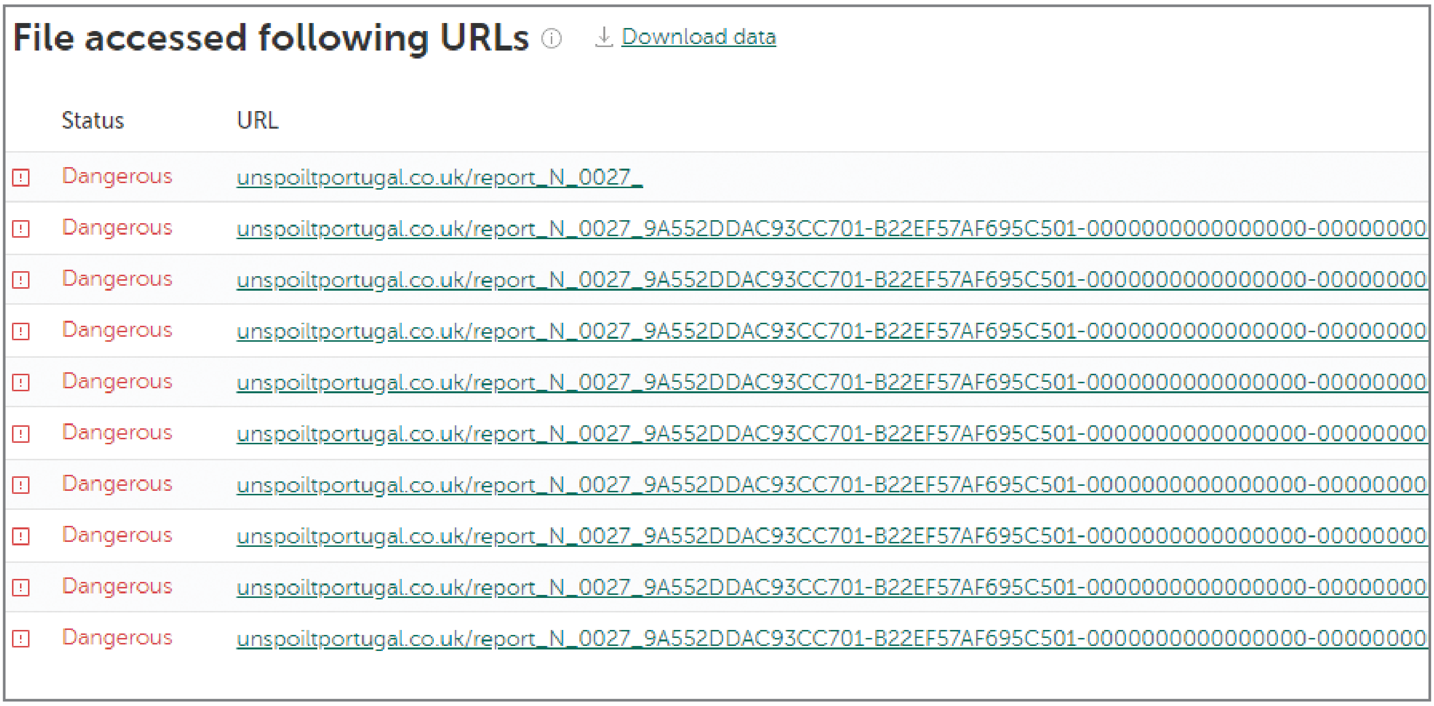
Classic sandbox capabilities would end at this point: you ran the file and you got the list of malicious activities — and that's all. But with the Kaspersky Threat Intelligence Portal, you can jump straight to the Threat Lookup to reveal more detailed intelligence on indicators of compromise and their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

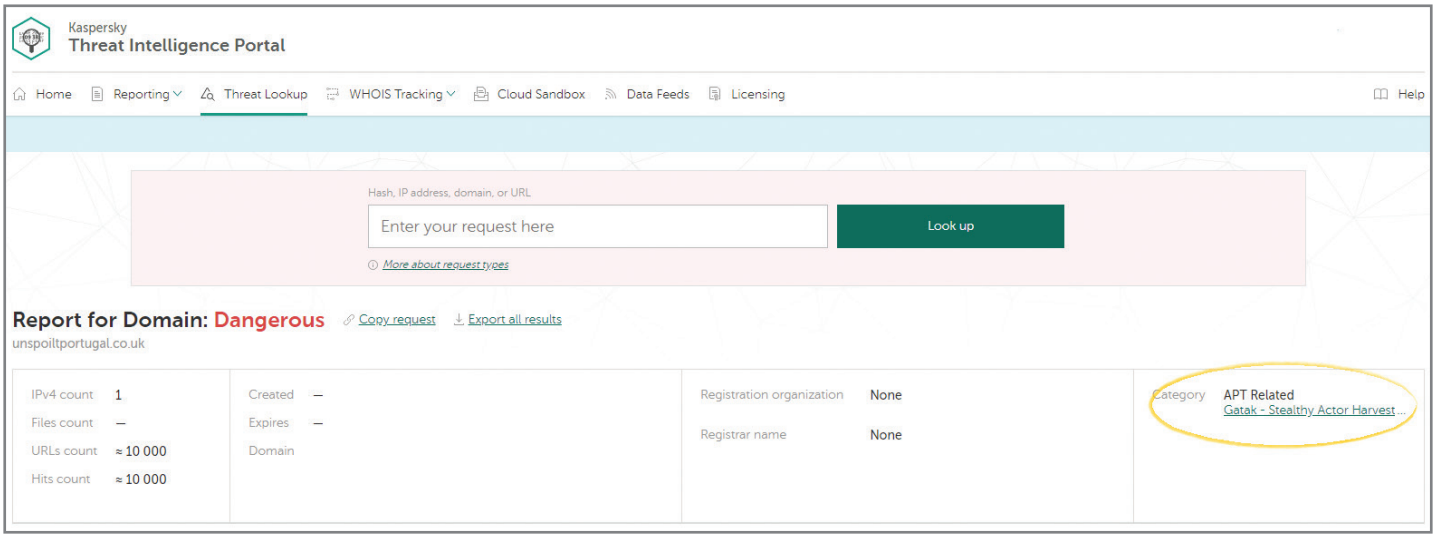
So, after we run our sample in the sandbox, we instantly use sandbox results as search queries for the Threat Lookup — just by clicking on the object (an MD5 hash in this case)



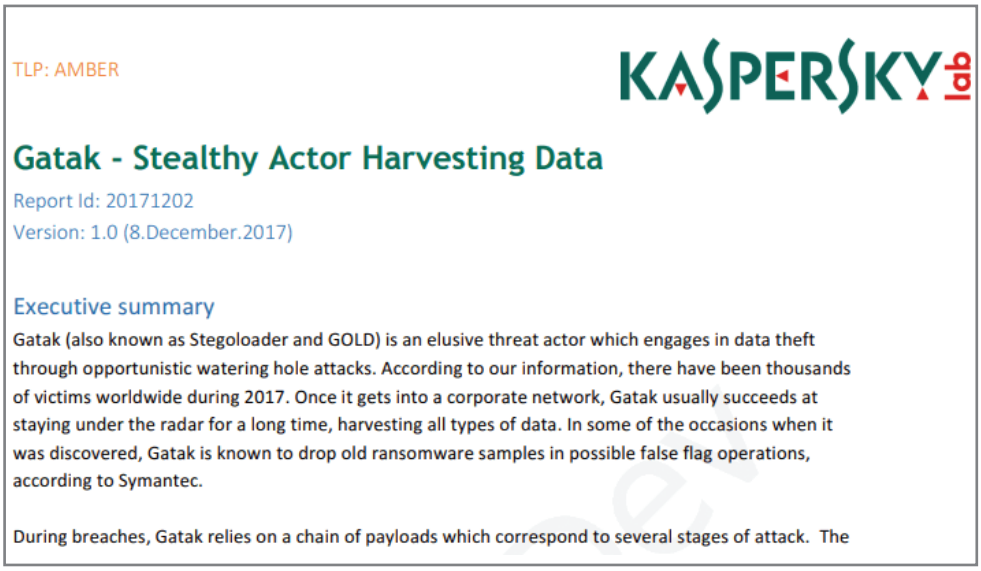
Now we have a more detailed report on the malware. Let's scroll through the Threat Lookup results to see which URLs were accessed by the malware we're exploring:



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:



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.


TLP: AMBER

KASPERSKY lab

Gatak - Stealthy Actor Harvesting Data

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

Executive summary

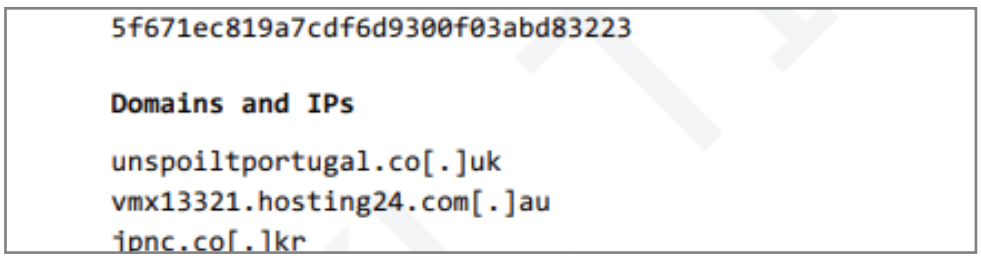
Gatak (also known as Stegoloader and GOLD) is an elusive threat actor which engages in data theft through opportunistic watering hole attacks. According to our information, there have been thousands of victims worldwide during 2017. Once it gets into a corporate network, Gatak usually succeeds at staying 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[.]lkr

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
IT Security News: business.kaspersky.com/

www.kaspersky.com

kaspersky BRING ON THE FUTURE