Stairwell

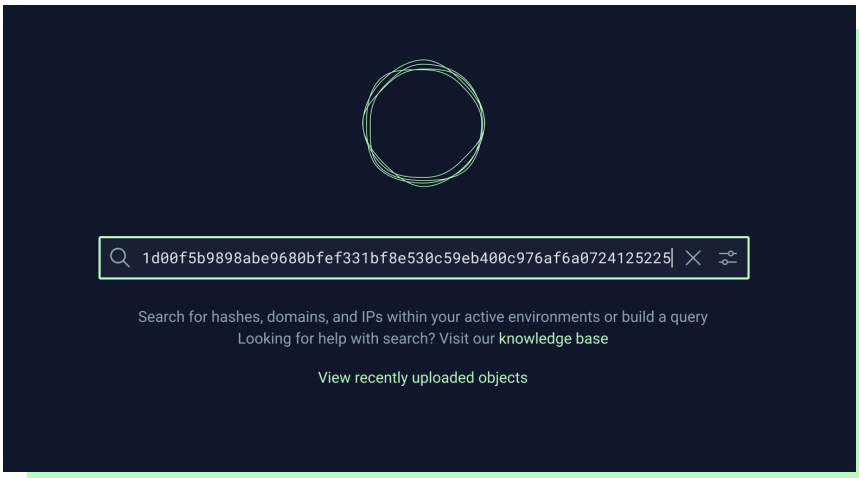
Malware variants are a big problem – but finding them doesn't have to be

Malware — malicious code that disrupts service, steals sensitive information, or gains access to private systems — is responsible for almost 40% of all breaches according to the 2022 Data Breach Investigations Report by Verizon. To avoid financial and reputation losses when you've identified malware in your organization's environment, response time is critical. You need to know what systems are impacted so you can immediately remediate them.

Because attackers are continually creating multiple variants to bypass defenses created for the original malware, you also need to quickly identify variants as they evolve. In fact, the Center for Internet Security reports that in 2022, the top 10 malware variants comprised 69% of total malware activity.

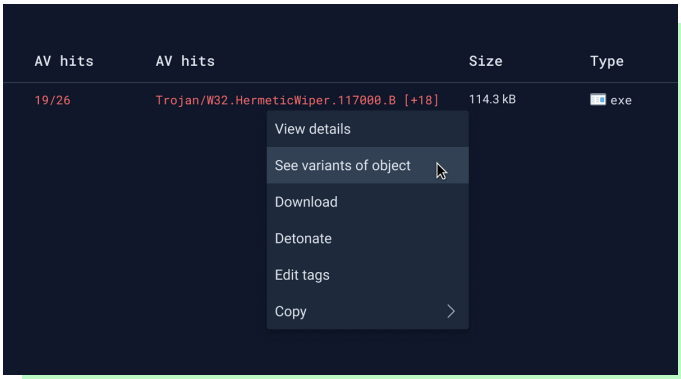
Inception identifies malware variants in seconds

It can take attackers a matter of hours to create malware variants that can get around the defenses for known malware. And, typically, it takes experts days or even weeks to discover those variants. With the Inception platform, however, you can immediately pivot from known malware to related malware in a matter of seconds.

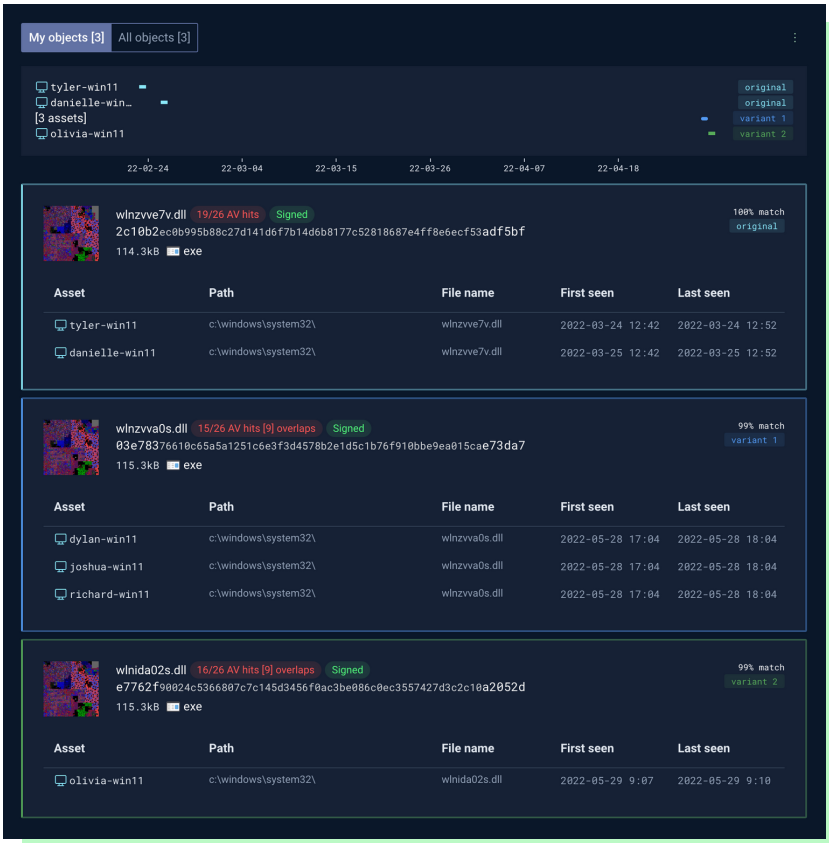


Here's an example of how it works in Inception's continuous intelligence, detection, and response process. First we'll run a query to see if HermeticWiper exists in our environment. We'll search for it using indicators of compromise copied from a blog about it.

Malware variants are a big problem – but finding them doesn't have to be



Inception tells us that HermeticWiper is present in the environment! To determine whether there are also any variants of the malware, simply right-click on the file and select See variants of object as shown below.



In seconds, the Inception platform discovers two variants of HermeticWiper with a 99% confidence level. You can see the date and time each variant entered the system and the machines affected.

The timeline view gives you insight into when the malware or variant was first seen and how it spread.

You can create an alert for each variant with a YARA rule.

You can also use the Variant Discovery API to find variants flagged by other security tools, such as your EDR. With an API call, Inception will return hashes of the variants and the confidence of the finding.

Try the Inception platform and variant discovery for yourself; contact us at stairwell.com.

Stairwell