

Antivirus and EDR



Antivirus and EDR Components

Kernel-mode drivers

Callback routines,
filter-drivers, network
drivers

User-mode services

Collects telemetry,
communicates with
cloud services

API monitoring

API monitoring to get
extra insight into
process activity

ETW

Consume events from
ETW providers to
collect telemetry

Emulators & Sandboxes

Emulate or execute files
and scripts to identify
malicious activity

AMSI providers

Scan scripts at runtime
to prevent malicious
activity



Kernel-mode Drivers

Callback routines

- Process operations
- DLL loading operations
- Thread operations
- Handle operations
- Registry operations

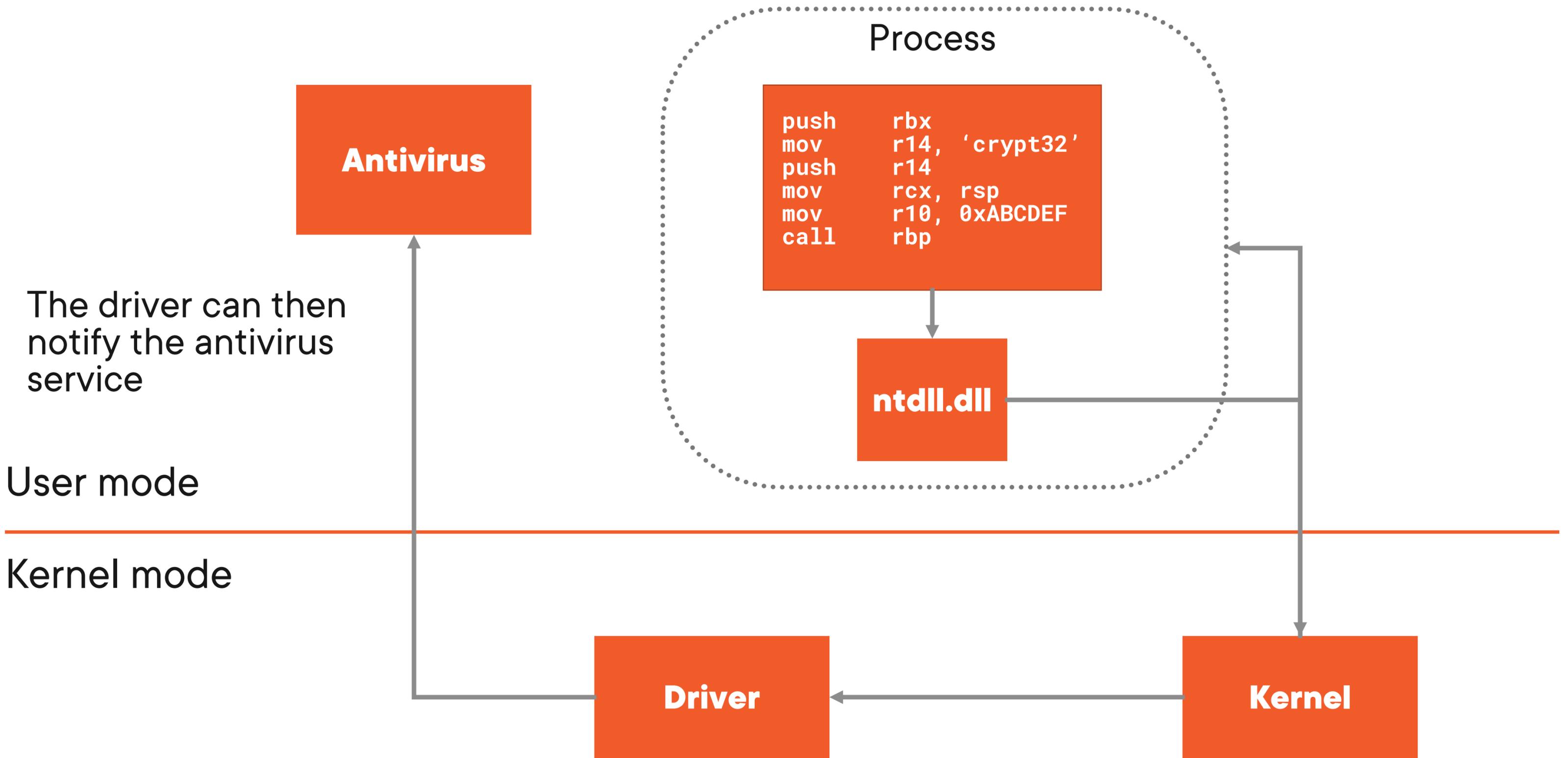
Filter drivers

- File-system activities

Network drivers

- Network activities





The driver can then notify the antivirus service

User mode

Kernel mode

The Kernel notifies the driver by calling its registered callback function



API Monitoring

Usually a DLL that uses a hooking library such as Microsoft Detours

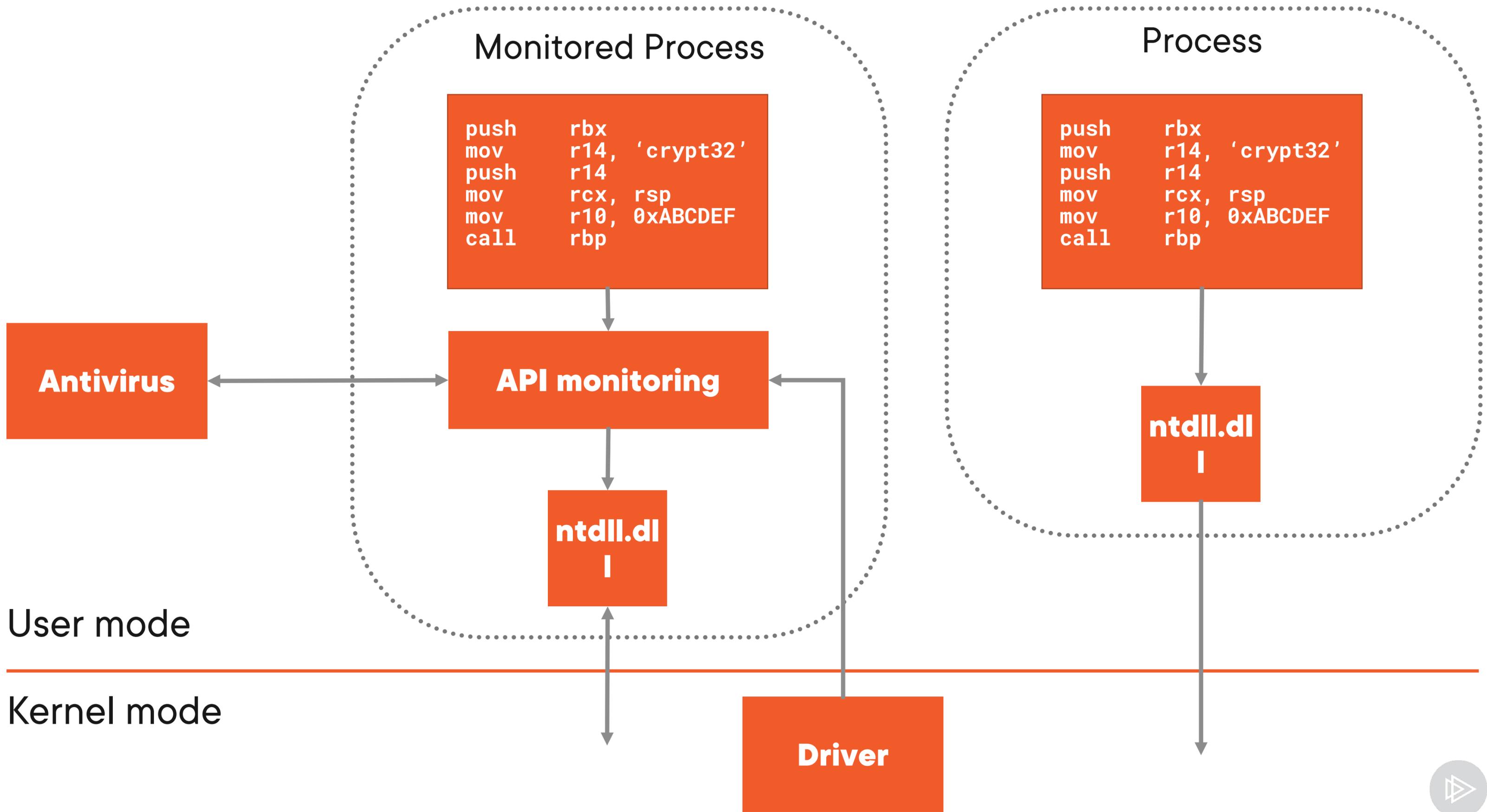
Injected by Kernel-mode drivers when processes are created

Gives the Antivirus visibility into a process's runtime behaviour

Hooks frequently abused API functions

- GetProcAddress
- VirtualAlloc
- LoadLibrary
- WriteProcessMemory
- CreateRemoteThread





ETW

Provides additional telemetry

Microsoft-Windows-Threat-Intelligence

Memory and thread operations

More robust than API monitoring



Emulators

Emulates an executable file or script to figure out what it would do if executed

Tries to make the executable file or script believe they are being run on a real operating system

Artifacts are collected and may trigger a detection by the antivirus

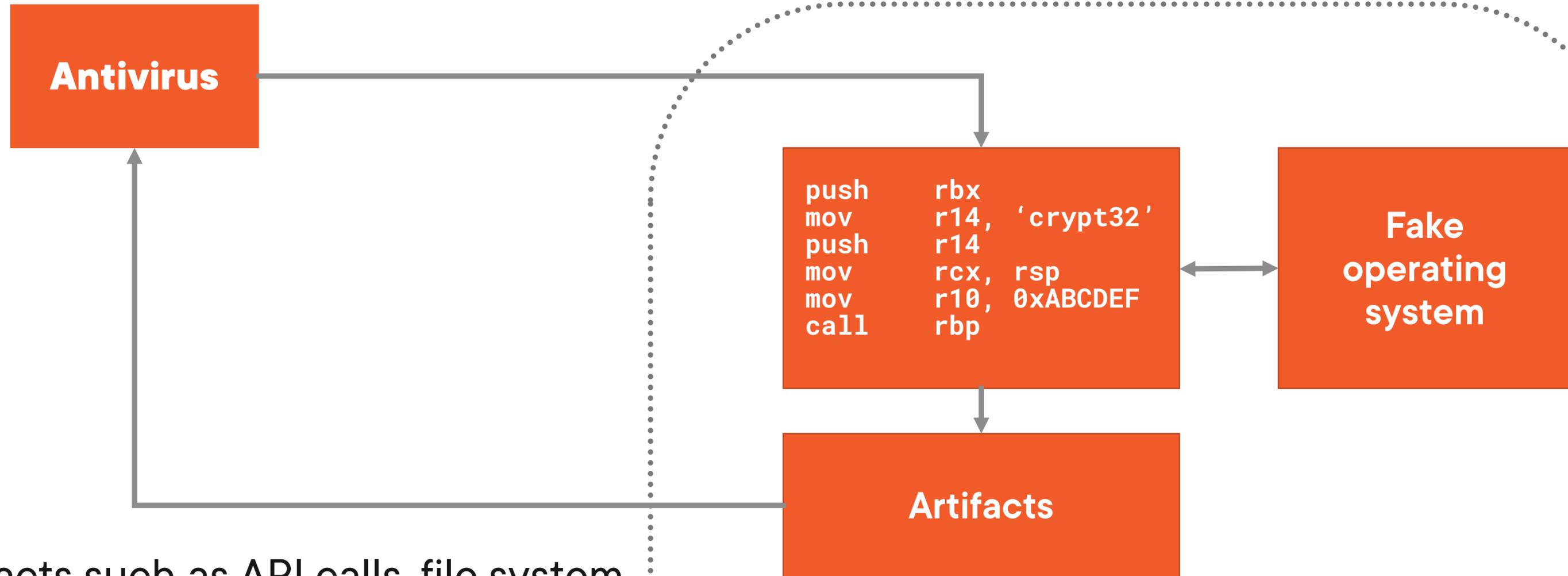
Emulation is expensive and usually has a termination condition

- **Number of CPU instructions emulated**
- **Elapsed time**
- **Number of API calls identified**



Executable file or script is sent to the emulator for analysis

Emulator



Artifacts such as API calls, file system access, registry access and memory dumps are sent back to the antivirus for analysis

Instructions are emulated in a fake environment which tries to mimic a real operating system



Sandboxes

Usually a Cloud-only feature due to performance impacts

Uploads an executable file or script to the Cloud for analysis within a sandbox

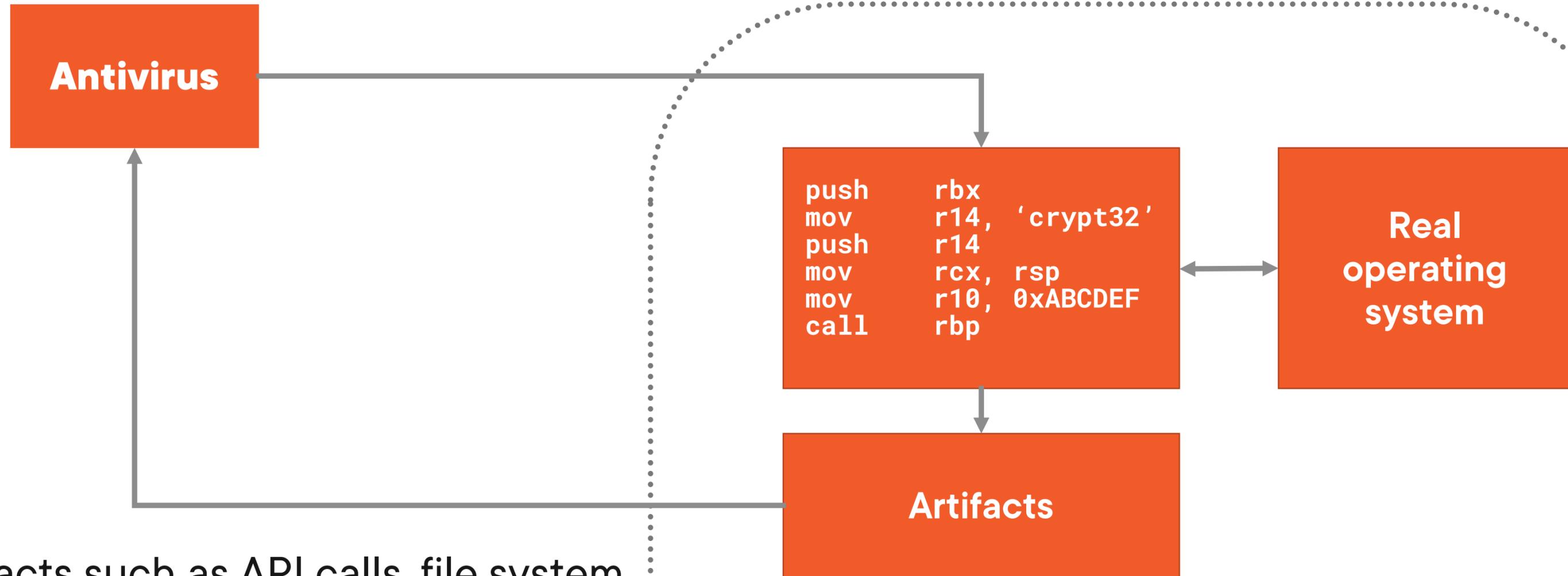
Differs from emulation because the file or script is executed

Artifacts are collected and may trigger a detection



Executable file or script is sent to the sandbox for analysis

Sandbox



Artifacts such as API calls, file system access, registry access, memory dumps, network connections and Screenshots are sent back to the antivirus for analysis

Executable file or script is executed on a real operating system.



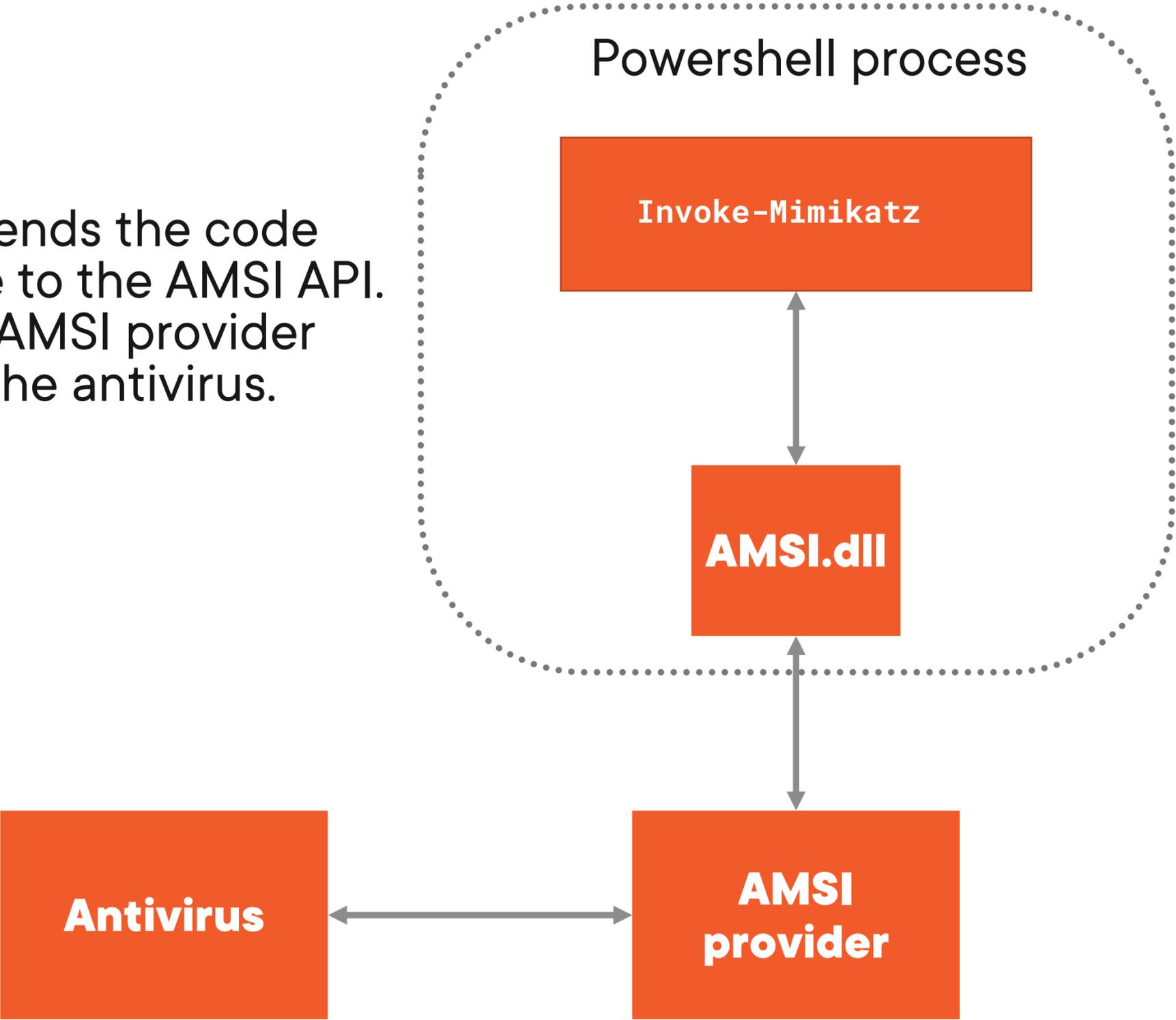
AMSI Providers

Scan scripts at runtime

Useful to get insight into a script at runtime



The Powershell process sends the code that it is about to execute to the AMSI API. The API will then call the AMSI provider which was registered by the antivirus.



User-mode Services

Consolidates and correlates the telemetry from the different data sources (Drivers, API monitoring, emulators, ETW consumers, AMSI etc...)

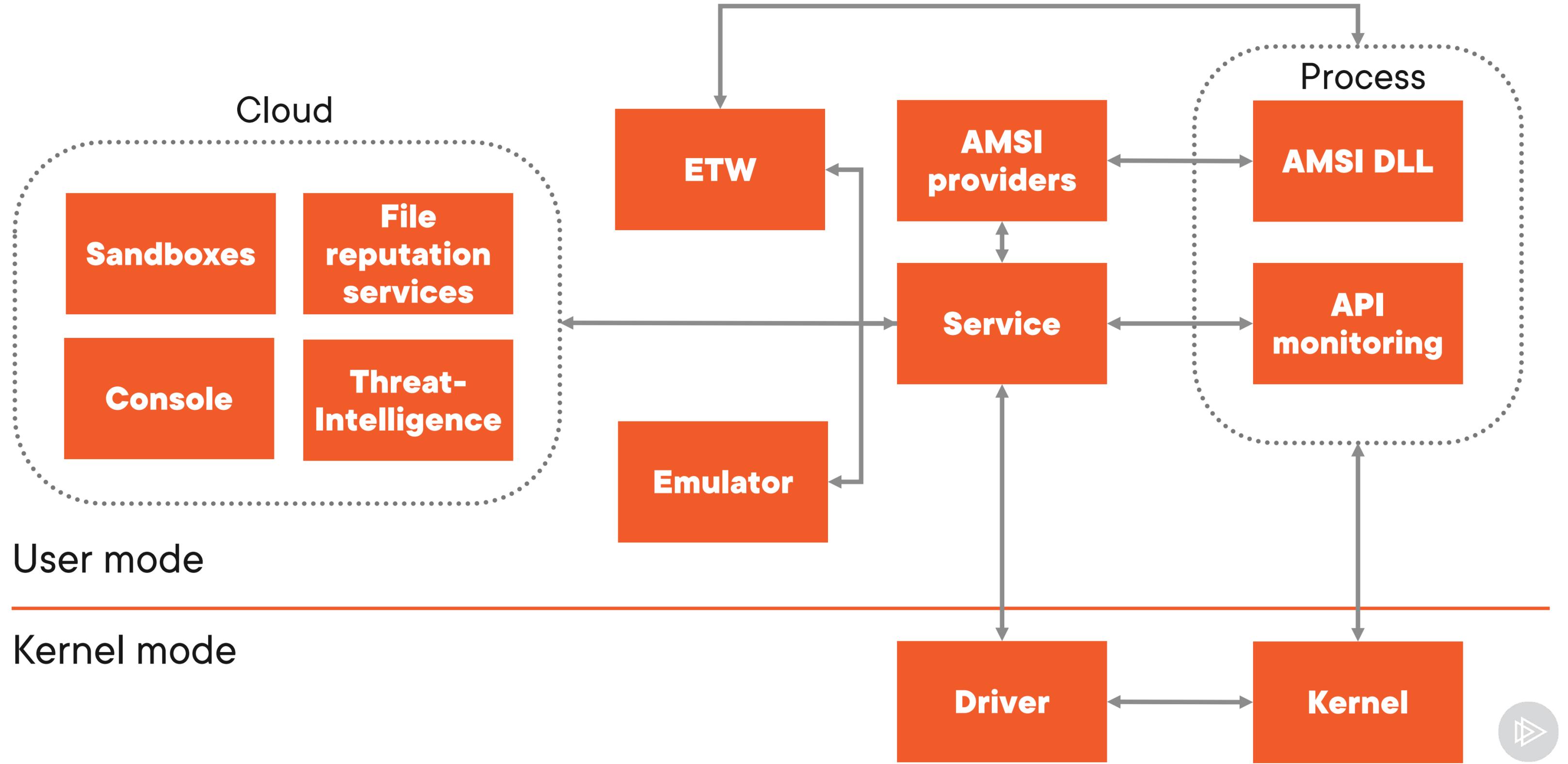
Orchestrates the antivirus activities

Triggers file analysis and scans

Sends files and scripts to emulators

Sends the telemetry to central monitoring consoles, cloud-based file reputation services and sandboxes so that it can be correlated with threat-intelligence data feeds





Antivirus and EDR Detections

Signatures

Match a specific sequence of bytes on disk, in memory or on the network

Hash

A file being written to disk matches a known malicious file hash

Heuristics

A process is behaving in a way which is likely to be malicious

ML classifiers

A file is classified as malicious because of its characteristics

Threat-Intelligence

Known malicious file names, IP addresses and domain names

