REASON CORE SECURITY

Anti-Malware SDK

The Reason Advantage

- Protects users from adware and PUPs
- Scanning and real time protection
- Modern native libraries to accelerate the development process
- Easy to integrate
- A rich set of client and server-side functionality for adding malware protection to your codebase
- Lightweight footprint; requires minimal system resources
- Provides full and flexible control to developers
- The SDK provides a single integration point to many of Reason's security technologies.
- Detect, disable and remove potentially unwanted applications
- Highest potential coverage in the industry

The threat of malware is growing at an astounding pace and in accordance, the anti-malware market has ballooned tremendously. While most anti-malware and antivirus software solutions address one main issues, malware, (which is a combination of trojans, worms, viruses, rootkits and spyware) most stay away from addressing the massive increase of adware and PUPs (potentially unwanted software) that infest users at an ever growing rate. Reason's security products tackle adware and PUPs head-on with market leading analysis and detection, which no other vendors in the market come close to currently. Reason is proud to extend our core platform technologies to developers and OEMs to help them protect their users from adware threats.

01.
Cloud SDK

Integrate Reason's Anti-Malware SDK Into Your Product or Service

Reason's Anti-Malware SDK allows your company to integrate an anti-malware (adware and PUP) solution into Windows software using a set of simple interfaces to provide comprehensive protection and analysis from many types of internet threats, including: adware, potentially unwanted programs (PUPs) trojans, worms, spyware, and other malware intrusions. Used by top security products with over 500,000 daily installs, Reason's SDK is the combination of the latest anti-adware, PUP and malware technologies. We provide supreme detection and one of the lowest false positive rates, while ensuring instant reactions to adware threats.

Overview

Reason's Anti-Malware SDK is a robust, feature-packed, and multi-layered security framework for building Windows security software, or for adding adware and PUP protection into existing anti-malware applications. Reason's Anti-Malware SDK is an award winning malware protection engine for Windows that can be integrated into existing or new OEM products to protect users against adware and PUPs (potentially unwanted programs), as well as all forms of malware including trojans, worms and spyware. Our SDK provides both scanning and real-time protection technology in a transparent and easy to integrate solution. To use it, simply drop the engine SDK into an application and with a few API calls you can protect your users from many types of malware threats. With a very strong focus on adware and PUP protection and an extremely lightweight footprint, you can run the anti-adware SDK alongside existing anti-malware solution to provide protection where other AV's don't.

The Reason Anti-Malware SDK provides partners with full, but flexible control over branding and user interface implementation. The SDK is lightweight and efficient and utilizes little memory and bandwidth, while maintaining minimal impact on system resources. Developers have full control and flexibility over the how the elements are implemented.

02.
How to use

Who Should Use the Reason SDK?

There are two primary categories of app developers who utilize the Reason SDK:

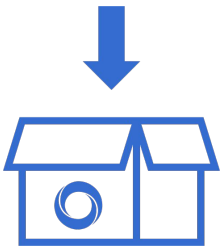
1. Established security companies: Existing security companies such as anti-malware and anti-virus products focus all of their energy in protecting users from truly hard to find and remove malicious threats such as viruses and rootkits. This leaves them little time to go after the huge adware and PUP market where things are not so black and white. While most companies have large labs and conduct extensive research to find malware, they lack the resources to handle the ever-changing world of adware. Reason's adware-focused solution helps these companies apply their talents to finding and dealing with really nasty malware, while the SDK does the adware-hunting dirty work.

2. Novice security software developers: Adware and PUPs continue to be a major issue on Windows, and many developers want to develop security software addressing these issues but developing proper security products isn't easy. It takes vast expertise and resources to identify and fend off consistent adware. Most developers are not security experts, nor do they need to be. They want to work with a turnkey solution that provides the security component. Doing so allows them to use their expertise to build a differentiated and compelling front end.

03.
How it works

How it Works

The Reason Anti-Malware SDK is a small file (just a couple megs). It requires minimal system resources, particularly when compared to a traditional security and anti-malware SDKs. Yet, Reason's SDK has the highest potential coverage in the industry. The SDK offers different features that developers can draw upon to include within their products. By integrating these protection features into their Windows programs, developers can protect their users from the latest adware and PUP threats.



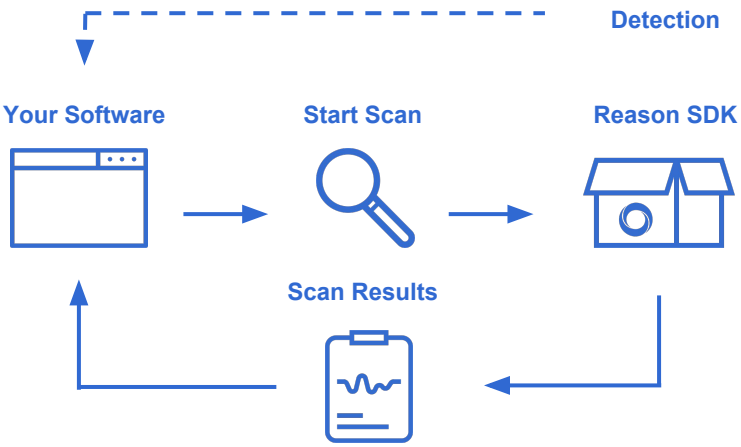
Reason Anti Adware SDK:

- Scanning
- Real-time Protection
- Quarantine
- Bundle Protection
- URL Scanning

The SDK itself is implemented in two forms: a robust full-featured API that can be accessed through a number of programming languages including .Net, or through a comprehensive command line interface. The choice is entirely up to the developer, as both interfaces support most of the same features.

1. Scanning

Reason provides APIs for scanning files and other objects either individually, by set, or through various pre-defined structures (folders, quick scanning, deep scanning, full scanning, auto-start scanning, process scanning, memory scanning, etc.). Comprehensive details will be furnished based on the scan results. In addition, triggers and events can be consumed throughout all stages of the scanning process.



03.
How it works

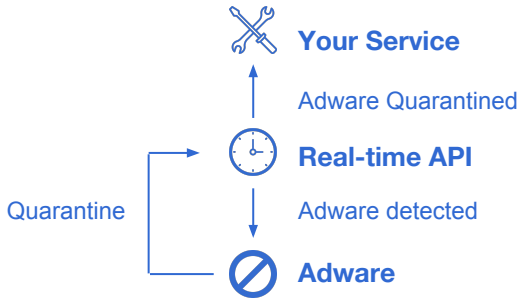
The API and Reason scanning engine will scan the following objects:

- Files (PE, scripts, all other file types)
- Executing processes and all loaded process memory, injected code and handles.
- ASEPs (All auto-starting execution points, 180 unique points that include everything from services and drivers to powershell scripts, etc.)
- Browser settings, extensions and plugins (IE, Edge, Chrome, Chromium, Firefox, Opera)
- A number of other ways adware takes advantage including hosts, proxies and many more.

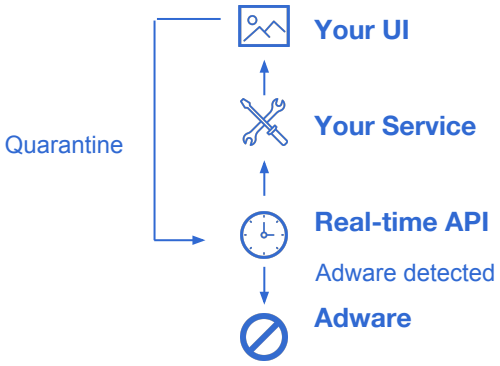
2. Real-time Protection

Once enabled, depending on the specified parameters, the real-time protection API will automatically detect new adware objects in real-time and apply removal actions or report findings for later handling to the software. With dozens of specific settings, real-time protection can be built around your exact requirements. The real-time protection API can be implemented as an existing library in any type of long running process, such as an existing or new Windows service, or can be run through various mechanism via the command line component. The real-time protection API provides a flexible implementation as well as a bounty of features to extend the level and kind of protection you can incorporate into your products. Ranging from a fully automated solution in which the API is set up to automatically handle all detected adware, down to a more granular approach in which the developer provides a robust set of interaction mechanisms to control the generality - as the developer, you set the parameters for functionality. For example, you can configure settings to automatically remove any detected adware (or malware), or you can simply consume events from the API where, if new adware is detected, the API will throw events asking your software how to handle it, while giving you the necessary information required to make a decision. In the latter case, you can then make the decision to remove the detected objects by telling the quarantine to handle them, or you can have the API lock the objects and throw any custom UI you would like to the end user, allowing them to make a decision.

Minimal Interaction



Full Interaction



3. Quarantine

Once adware, PUPs or other malware are detected, the Quarantine API will handle disposing, removal and cleaning of such objects. Reason's advanced removal technology will make sure that all aspects of an object are completely removed from the system. This includes all connections to an object from registry entries to ASEPs (auto-start execution points), including memory hooks and other integration points. When an object and its parts are quarantined from the system, the Quarantine API can restore these objects at a later date if required.

4. Bundle Protection

Our proprietary bundle protection solution is a set of APIs and services that prevents users from checking unwanted offers and downloading potentially unwanted programs (PUPs) while installing software.

5. URL Scan

The URL scan API enables your product to protect users from phishing and malicious web sites, including download sites that serve adware and PUP installers by scanning the threat level of a given URL or domain.

6. Browser Extension Scan

With this API, you can check the risk of a given Chrome/Chromium, Firefox or Microsoft Edge extension based on various parameters. These parameters include the packaged extension for XPI and CRX packaged extensions, the manifest.json or install.rdf or the extension IDs. The Reason API keeps an extensive list of bad extensions based on various factors, including, but not limited to, malicious or unwanted browser asset takeovers. Developers can then leverage this API to prevent or remove potentially unwanted extension from taking over a user's web browser. Like all other API features, once a determination is made, the Quarantine API can then be used to safely remove the extensions from the browser.

04.
Integration

How Integration Works

The current version of the Reason Anti-Malware SDK comes in two kinds and you can use a combination of both to meet the needs of your development criteria. These versions include an extensive API that can be integrated using a variety of languages, including .Net or C++, as well as a robust command line interface that's language agnostic. In terms of distributing the SDK, you can elect to use our silent installer which will drop the required SDK components, or you can package and install the individual files on the client's device utilizing your current installer. In either case, we have extensive developer documents and sample projects to help jump-start your development integration.

Example command line call to scan a single file

This will scan a single file and write the results in XML format to standard output as well as output the same results to a file.

```
rsEngineCmd.exe -scan -type=quick -apikey={APIKEY} -verbose
-output="C:\output.xml" -verbose -console=xml
```

Example command line call to run a quick scan

This will run a quick scan and write the results in JSON format to standard output.

```
rsEngineCmd.exe -scan -type=custom -paths="c:\sample.exe"
-apikey={APIKEY} -verbose -console=json
```

Example API call using C# to run a quick scan

(This is a very simplified pseudo-code implementation)

```
Using Reason.rsEngineSDK;
static void Main(string[] args)
{
 //Initialize the SDK client. This is required to utilize the
SDK.
        Client.initialize("1111-1111-1111-1111");

        //Setup a scan and subscribe to the events
        Scan.ScanProgressEvent += Scan_ScanProgressEvent;
        Scan.ScanDetectionEvent += Scan_ScanDetectionEvent;

        //Execute a quick scan.
        Scan.ScanResults oScanResults =
Scan.scan(Scan.ScanTypes.Quick);

        //Do something with the ScanResults.
        if (oScanResults.ScanDetectionsCount > 0)
        {
            //Adware was detected. Enumerate all detected
```

04.
Integration

```
            foreach (Scan.ScanResults.ScanDetection oScanDetection
in oScanResults.ScanDetections)
            {
                Console.WriteLine("Detection: " +
oScanDetection.Name + ")");
            }
        }
        else
        {
            //Malware was not detected.
            Console.WriteLine("You do not have any malware on your
computer.");
        }

        //Remove subscribed events
        Scan.ScanProgressEvent -= Scan_ScanProgressEvent;
        Scan.ScanDetectionEvent -= Scan_ScanDetectionEvent;
}

static void Scan_ScanProgressEvent(int percent, string details)
{
      Console.WriteLine("[" + percent.ToString() + "%] " + details);
}

static void Scan_ScanDetectionEvent(string detection, string details,
string path)
{
      Console.WriteLine("Detection: " + detection + " (" +path +
")");
}
```

05.
About

About Reason Software Company

With a very strong desire to change the way the anti-virus industry has been operating for the last 30 years, we bring a revolutionary approach to threat detection. By leveraging cloud computing and big data analytics, we provide PC users with the fastest and most accurate protection available on the market today. Our SDK is designed to work along side traditional anti-virus products and attack threats that most AVs don't touch.

Since 2012, Reason has brought our unique approach to design and development with other amazing products, including Boost and the award winning Should I Remove It?, serving tens of millions of happy users. Reason products have been featured by CNET, PCWorld, The Next Web, Discovery Channel, Kim Komando, USA Today and hundreds of other media outlets and blogs.

06.
Contact

How to Contact Reason's SDK Group

Phone:
646-664-1038 ext 600

Email:
oems@builtwithreason.com

Address:
Reason Software Company Inc.
228 Park Ave S #74122
New York, NY 10003-1502