Anti-Virus File Reputation Services

In today's netspeed environment, traditional antivirus protection is not enough. The majority of antivirus products rely on signature or hash-based methods of detecting "known-bad" activity or files. Unfortunately, small modifications to malicious files and innovative malware techniques easily defeat this approach. By introducing a more informed discovery process, Antivirus Cloud Lookup capabilities provide protection during the gap between detecting a threat and deploying signatures.

What is Antivirus Cloud Lookup?

Antivirus Cloud Lookup, also known as File Reputation Lookup or Cloud Heuristics, is a recent advancement in antivirus technologies that leverages a remote, cloud-based centralized infrastructure that compiles information on file reputations. File reputation is the likelihood of a file or executable being maliciousbased on its characteristics and activities.

The AV Cloud infrastructure contains the latest signatures from the AV vendor's database as well as data gathered from millions of clients around the world. Antivirus clients can reference the global reputation database to discover potentially malicious files running on its host machine.

Benefits

AV Cloud Lookup offers several benefits:

- Provides more complete coverage than the corresponding base antivirus product alone and offers optimal protection in connected and disconnected environments when used in conjunction with the base antivirus product.
- Initiates protection against newly discovered malware within seconds versus the hours or days required for updating signature files. Conversely, the discovery of malicious activity on one client will populate the central reputation database that protects other clients.
- Provides mechanisms for increased controls over every file entering the network, helping to control network hygiene.
- Has a low false positive rate compared to traditional signature-based techniques alone.
- Although this document only addresses file reputation lookup, many vendor cloudbased reputation capabilities offer additional services such as IP address or website address reputation.

Risks

There are several potential risks and concerns when it comes to employing AV Cloud Lookup. Some of these risks originate from the use of traditional signature-based antivirus products and are not unique to the AV Cloud Lookup.

False Negatives

An adversary deceives the antivirus product into believing a malicious file is safe.

In order to create a false negative, the adversary must employ a technique such as a man-in-the middle attack that compromises network infrastructure by redirecting or blocking traffic coming to and from the reputation database. False negatives leave systems vulnerable because malicious files might be executed.

In most cases, the overall risk is not increased by the use of Cloud-based Lookup.

False Positives

An adversary deceives the antivirus product into believing that a critical good file is actually a malicious file.

In order to create a false positive, the adversary must use a technique that modifies the reputation of the good file to appear to be malicious by compromising either the global reputation database or the queries between the client and global reputation database. False positives may delete critical good files or prevent them from

executing on the system, causing denial of service for systems or programs referencing those files.

The cost of developing such compromises is high, which lowers the overall risk. Moreover, the ability to exclude critical files from scans is a common feature of AV Cloud Lookup products.

In addition, the reliability of reputation mechanisms are directly related to how common files are in the global network. In general, you may need to exclude uncommon, but approved files (e.g. custom or specialized software) from scanning in order to avoid generating false positives.

Disclosure

An adversary examines the queries made by clients for valuable information.

In order to gain valuable information, the adversary would need full view of queries as they cross the Internet. A full view of the queries would reveal the data or metadata of the clients using the antivirus product.

However, the overall risk of disclosure is low since AV Cloud Lookup products use obfuscation or encryption in the traffic to their reputation databases.

Implementing AV Cloud Lookup

AV Cloud Lookup is often included in several major antivirus products as an optional service (e.g. products from McAfee®, Symantec®, Blue Coat®)[1]. Most vendors recommend initially configuring file reputation sensitivity at a "medium" setting, though sensitivity can be adjusted for the needs of a given network.

Contact Information

Industry Inquiries: 410-854-6091

USG/IC Client Advocates: 410-854-4790

DoD/Military/COCOM Client Advocates: 410-854-4200

General Inquiries: **niasc@nsa.gov**

[1]McAfee® is a registered trademark of McAfee, Inc. Symantec® is a registered trademark of Symantec. Blue Coat® is a registered trademark of Blue Coat Systems, Inc.