


Quarantine **CONFIGURATION**



THREE CONSIDERATIONS
FOR FILE QUARANTINE
CONFIGURATION

Introduction

When dealing with potentially malicious files, a digital quarantine has the same goal as a physical one; isolating the infection can prevent it from spreading and compromising other healthy individuals. Once the potential threat is isolated, forensic analysis can be done to determine the exact cause or source of the threat that has been quarantined, however long it takes to complete the analysis. After the threat has been analyzed, it can be released, neutralized, or removed depending on the conclusions of the analyst(s).

Advantages of File Quarantine

When malware is suspected in digital files, there are significant advantages to quarantining them instead of removing anything that is identified as a potential threat. The first is that the chance of misidentifying a harmless file as malicious (a false positive) can never be completely eliminated. If that file is permanently deleted, valuable data may be lost without the possibility of recovery. Quarantining the file instead allows for the possibility of restoring that file if it turns out not to be a threat.

A second advantage of quarantining a file instead of deleting it emerges when a real threat is identified. It is valuable to examine the file to determine its source; if the origin of the malware is identified either legal or technical action can be taken against that malicious actor. Forensic analysis can also find out more about the threat and use that information to identify or block similar threats that would not have been detected otherwise. This is especially true in the case of new and unique threats.

Considerations for Quarantine Configuration



1. When should the quarantine occur?

If files are being checked at the entry point to a secure network, for instance, a quarantine can be used to hold onto any files that are potentially dangerous before they are allowed into the secure area. These files can then be analyzed using an organization's secure data workflow policies to determine whether they should be allowed entry, sanitized to remove embedded threats, held for further analysis or deleted. Because the file is being held in the quarantine, there is an opportunity to gather more information about the file if it is needed to make a final decision. The source of the file could potentially be queried for more data, or additional systems could be used (such as dynamic analysis engines) to help clarify whether the file should be allowed.



2. What do we do when threats are detected?

A key decision that needs to be made when defining a security policy is what to do if malware or other threats are found inside a secure network. One might assume that if entry to a secure network is controlled, then any data that has passed those checkpoints should be free of threats. In reality, there are many reasons that a malicious file could be found within a secure network.

The first might be that files were introduced in such a way that they circumvented the security checkpoints in place. For example, end users could accidentally bring in USB devices without first scanning them to see if there were any threats. Another possibility is that new threats often pass undetected for a period of time before they are identified as malicious by the security defenses in place. If a threat is brought in during this delay in detection, it could then

enter the secure network and still be active even after the perimeter security checks are updated and are detecting it as a threat.

If such malware has been identified, the quarantine policy should specify at which level the threat should be quarantined. The individual file could be isolated, or it could be more appropriate to isolate the entire system or network where that threat was found. This will depend on the environment where the threat is found, as well as the characteristics of the threat itself. For low-security networks, it may be enough to simply isolate the file until it has been examined. On systems that have access to critical networks, however, you may want to isolate the entire system so that it can be investigated and cleaned before it is again allowed access to the network. In extreme cases, it may even make sense to isolate an entire network to make sure that the threat doesn't spread.

The appropriate level of response depends not only on the type of system/network affected but also the type of threat found. Many anti-malware systems classify potential threats according to their confidence in the severity of the threat in question. Some files are known to be malicious or clean, other threats may look similar to known threats even if they have not specifically been identified as a threat, while others still may look completely different than either known malicious or clean files and, therefore, be flagged for further analysis.



3. Who holds the keys?

Another factor to take into account when defining a quarantine policy is who should have the right to assess the files that have been quarantined to determine whether they should be released or permanently deleted, as well as whether any further action is needed. This is also heavily dependent on the variables mentioned above, as well as on the roles assigned to particular users or groups of users. Users may need to have their privileges restricted

either due to their access to sensitive information or due to their technical ability to properly assess the severity of a threat. Organizations may also want to limit their potential liability by restricting the group of people who have access to potentially malicious files or sensitive content.

Conclusion

Overall the use of a quarantine allows security administrators to have increased control over analyzing security cases that are neither unambiguously malicious nor unambiguously benign. By allowing for a middle ground where potential threats are neither immediately removed, nor automatically allowed into a secure area, additional time is gained. Administrators can conduct further analysis of the threat and make a much more appropriate decision as to how to proceed. The additional configuration options add some complexity to defining and administering security policies, but the benefits of improving the response to potential threats should far outweigh the costs.



<http://www.opswat.com>

Disclaimer. © 2016. OPSWAT, Inc. ("OPSWAT"). All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. OPSWAT is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. Though reasonable effort has been made to ensure the accuracy of the data provided, OPSWAT makes no claim, promise or guarantee about the completeness, accuracy and adequacy of information and is not responsible for misprints, out-of-date information, or errors. OPSWAT makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.