McAfee Host Intrusion Prevention Content 4933

Release Notes | 2013-05-14

Below is the updated signature information for the McAfee Host Intrusion Prevention 7.0/8.0 content (version 4933)

New Signature:

[New] *Sig 6045: SMB Brute Force Attack*

Description:

- *This event indicates an attempt to brute force enumerate SMB password remotely.*
- *This signature is set to High at default settings.*
- *This signature will work only on HIPs 8.0 or above.*

Modification:

[Updated]*Sig 2829: Block Packet Sniffer*

Description:

- *This signature has been modified to enhance the protection.*

[Updated]*Sig 6001: Suspicious Data Sequence in Javascript*

Description:

- *This signature has been modified to reduce the False Positives.*
- *This signature has been reintroduced and set to Medium level.*

[Updated]*Signature 1001:* Windows Agent Shielding - File Modification

Description:

- *This signature has been modified to reduce false positives.*

[Updated]*Signature 1002:* Windows Agent Shielding - Registry Access

Description:

- *This signature has been modified to reduce false positives.*

[Updated]*Signature 1003:* Windows Agent Shielding - Process Access

Description:

- *This signature has been modified to reduce false positives.*

[Updated]*Signature 3908: Access Protection - Prevent creation of new executable files in the Windows folder*

Description:

- *This signature has been modified to reduce the false positives.*

[Updated]*Signature 3909: Access Protection - Prevent creation of new executable files in the Program Files*

Description:

- *This signature has been modified to reduce the false positives.*

[Updated]*Signature 2787: W32/Yunsip Infection*

Description:

- *This signature has been modified to reduce the false positives.*

[Updated]*Signature 6015: Suspicious Function Invocation - Target Address Mismatch*

Description:

- *This signature has been modified to reduce the false positives.*

[Updated]*Signature 6032: Suspicious Function Invocation - Target Address Mismatch*

Description:

- *This signature has been modified to reduce the false positives.*

[Updated]*Network IPS filter driver: FireNfcp.sys*

Description:

- *This Network IPS filter driver has been modified to remove a redundant API call which could cause infinite looping for some network packet inspections.*

How to Update

You need to check in the update package to the ePO Repository, and then send the updated information to the agents. Please refer to ‘Updating’ in Chapter 8 of ‘Host Intrusion Prevention Product Guide’