Carbon Black
Refining Virus Total Watchlist Entries

11-Dec-2013
Cb-Support@Bit9.com

# Introduction

The purpose of this document is to describe how to modify a Watchlist to remove known entries. This example utilizes the Virus Total Watchlist mainly because it's the list we get the most customer feedback on.  The goal is to allow you to filter out entries you're aware of and do not wish to report their existence in your network.

# Sections

## Create a Custom Watchlist

The first step is to create a custom Virus Total Watchlist specific to your organization.

1. Go to the Search->Binaries->Add Criteria and select "VirusTotal Score" entry.

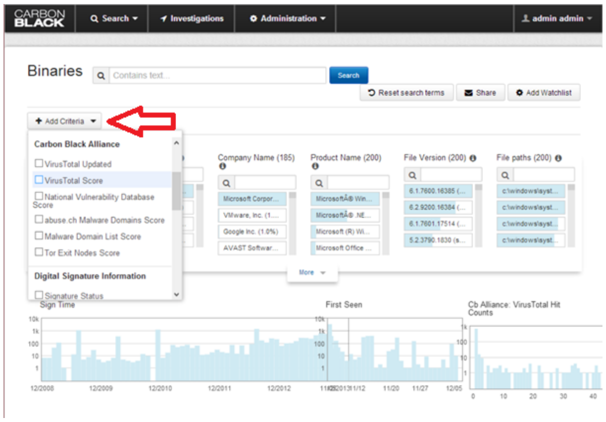
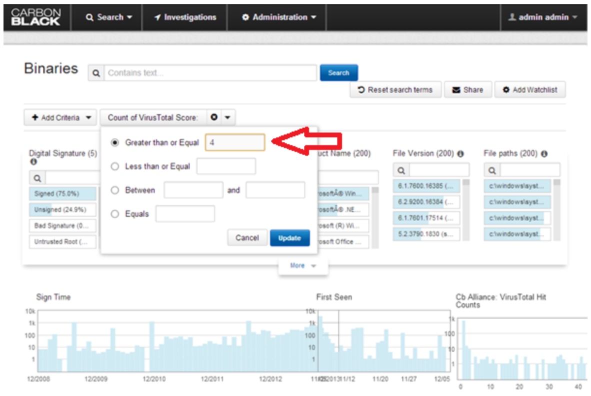


*Figure 1 Select Criteria*

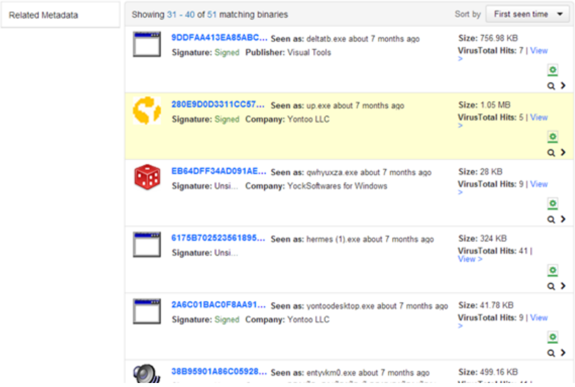
2. Enter the threshold for the minimum number of vendor hits to alert on.


Count of VirusTotal Score:

● Greater than or Equal 4
○ Less than or Equal
○ Between and
○ Equals

*Figure 2 Set Threshold*

3. Select the binary that you wish to exclude from reporting in the future. **Caution:** this binary will no longer be reported by this Watchlist.



Showing 31 - 40 of 51 matching binaries

9DDFAA413EA85ABC... Seen as: deltatb.exe about 7 months ago
Signature: Signed Publisher: Visual Tools
Size: 756.98 KB
VirusTotal Hits: 7 | View >

280E9D0D3311CC57... Seen as: up.exe about 7 months ago
Signature: Signed Company: Yontoo LLC
Size: 1.05 MB
VirusTotal Hits: 5 | View >

EB64DFF34AD091AE... Seen as: qwhyuxza.exe about 7 months ago
Signature: Unsi... Company: YockSoftwares for Windows
Size: 28 KB
VirusTotal Hits: 9 | View >

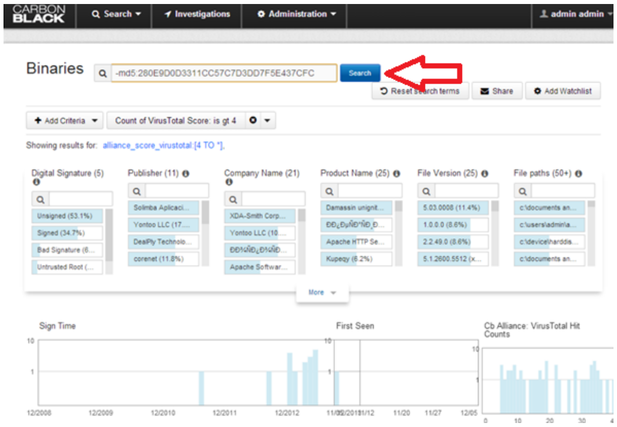
6175B702523561895... Seen as: hermes (1).exe about 7 months ago
Signature: Unsi...
Size: 324 KB
VirusTotal Hits: 41 | View >

2A6C01BAC0F8AA91... Seen as: yontoodesktop.exe about 7 months ago
Signature: Signed Company: Yontoo LLC
Size: 41.78 KB
VirusTotal Hits: 9 | View >

38B95901A86C05928... Seen as: entyvkm0.exe about 7 months ago
Size: 499.16 KB

*Figure 3 Find Binary to Exclude*

4. Enter the –md5:<hash value> into the search criteria box to prevent the hash from being displayed in the future.



-md5:280E9D0D3311CC57C7D3DD7F5E437CFC

Count of VirusTotal Score: is gt 4

Showing results for: alliance_score_virustotal:[4 TO *].

Digital Signature (5): Unsigned (53.1%), Signed (34.7%), Bad Signature (6..., Untrusted Root (...

Publisher (11): Solimba Aplicaci..., Yontoo LLC (17..., DealPly Technolo..., corenet (11.8%)

Company Name (21): XDA-Smith Corp..., Yontoo LLC (10..., ÐÐ¾ÑÐ¸Ð¾ÑÐ..., Apache Softwar...

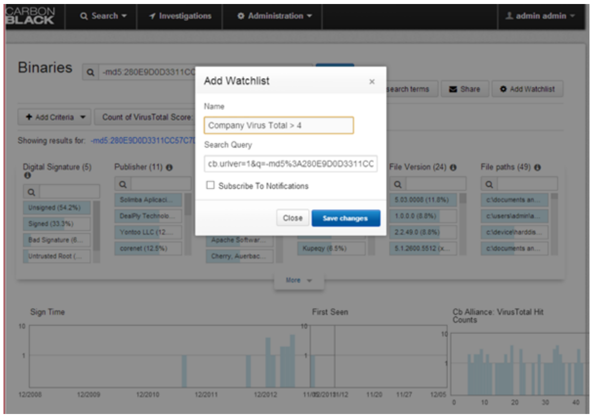
Product Name (25): Damassin unignit..., ÐÐ¿ÐµÑÐ°Ñ'ÑÐ¸Ð..., Apache HTTP Se..., Kupeqy (6.2%)

File Version (25): 5.03.0008 (11.4%), 1.0.0.0 (8.6%), 2.2.49.0 (8.6%), 5.1.2600.5512 (x...

File paths (50+): c:\documents an..., c:\users\admin\a..., c:\device\harddis..., c:\documents an...

*Figure 4 Enter Value to Exclude*

5. Name the Watchlist appropriately and save.



Add Watchlist

Name: Company Virus Total > 4

Search Query: cb.urlver=1&q=-md5%3A280E9D0D3311CC

☐ Subscribe To Notifications

Showing results for: -md5:280E9D0D3311CC57C7D

Digital Signature (5): Unsigned (54.2%), Signed (33.3%), Bad Signature (6..., Untrusted Root (...

Publisher (11): Solimba Aplicaci..., DealPly Technolo..., Yontoo LLC (12..., corenet (12.5%)

Apache Softwar..., Cherry, Auerbac...

Kupeqy (6.5%)

File Version (24): 5.03.0008 (11.8%), 1.0.0.0 (8.8%), 2.2.49.0 (8.8%), 5.1.2600.5512 (x...

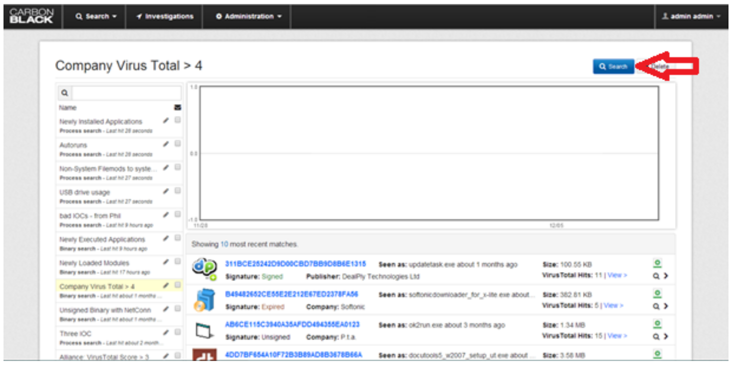
File paths (49): c:\documents an..., c:\users\admin\a..., c:\device\harddis..., c:\documents an...

*Figure 5 Save the Watchlist*

## Update the Watchlist

In this section we'll walk through the process to update a Watchlist to ignore additional binaries. Virus Total will sometimes alert on unwanted programs that you have authorized to be run in your environment. To prevent them continually alerting you on the Watchlist you can ignore them by prepending a "-" at the beginning of the key you wish to ignore and chain multiple values together with the conditional "OR" statement separating them. For example –md:<32-bits> OR –md:<32-bits> OR –md:<32-bits> etc… Keep in mind that larger list will decrease responsiveness of the UI due to additional processing requirements.

1. Expose the content from your Virus Total Watchlist created in the last section by selecting the search button.



Newly Installed Applications
Process search - Last hit 28 seconds

Autoruns
Process search - Last hit 28 seconds

Non-System Filemods to syste…
Process search - Last hit 27 seconds

USB drive usage
Process search - Last hit 27 seconds

bad IOCs - from Phil
Process search - Last hit 9 hours ago

Newly Executed Applications
Binary search - Last hit 9 hours ago

Newly Loaded Modules
Binary search - Last hit 17 hours ago

Company Virus Total > 4
Binary search - Last hit about 1 months …

Unsigned Binary with NetConn
Binary search - Last hit about 1 months …

Three IOC
Process search - Last hit about 2 month…

Alliance: VirusTotal Score > 3

Showing 10 most recent matches.

311BCE25242D9D00CBD7BB9D8B6E1315 Seen as: updatetask.exe about 1 months ago Size: 100.55 KB
Signature: Signed Publisher: DealPly Technologies Ltd VirusTotal Hits: 11 | View >

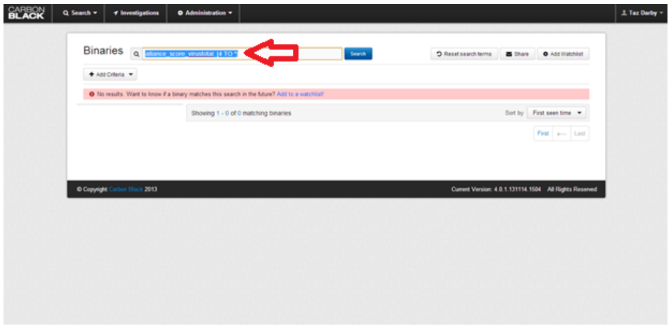
B49482652CE55E2E212E67ED2378FA56 Seen as: softonicdownloader_for_x-lite.exe about… Size: 382.81 KB
Signature: Expired Company: Softonic VirusTotal Hits: 5 | View >

AB6CE115C3940A35AFDD494355EA0123 Seen as: ok2run.exe about 3 months ago Size: 1.34 MB
Signature: Unsigned Company: P.t.a. VirusTotal Hits: 15 | View >

4DD7BF654A10F72B3B89AD8B3678B66A Seen as: docutools5_w2007_setup_ut.exe about… Size: 3.58 MB

*Figure 6 Expose Watchlist Query*

2. The original query string should look something like *alliance_score_virustotal: [4 TO *] OR –md5:<32-bits>* unless this isn't your first modification. Copy this value to your clipboard to allow addition of new conditionals.



alliance_score_virustotal: [4 TO *]

No results. Want to know if a binary matches this search in the future? Add to a watchlist!

Showing 1 - 0 of 0 matching binaries

© Copyright Carbon Black 2013 Current Version: 4.0.1.131114.1504 All Rights Reserved

*Figure 7 Copy Watchlist Query*

3. Add the MD5 value you want to exclude by prepending the minus symbol in front of the item you wish to suppress and the appropriate conditional. Press the search button to ensure the results are what you intended.

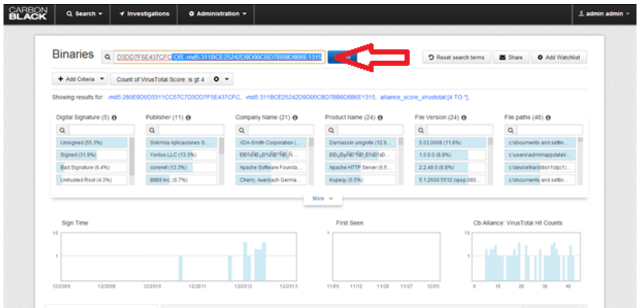
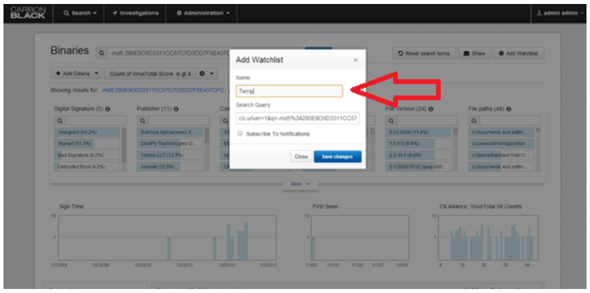


*Figure 8 Insert Updated Query String*

4. Save the new Watchlist with a temporary name.


Add Watchlist

Name: Temp

Search Query: cb.urlver=1&q=-md5%3A280E9D0D3311CC57

□ Subscribe To Notifications

*Figure 9 Save to Temporary Watchlist*

5. Select the Watchlist to verify it is working correctly.

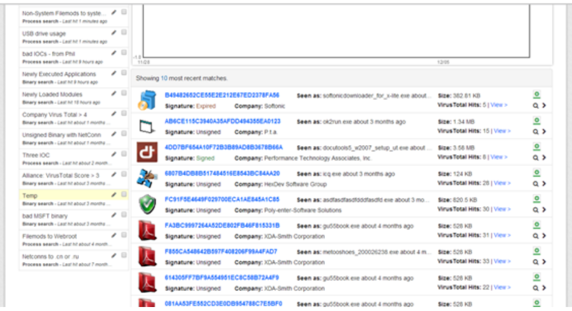
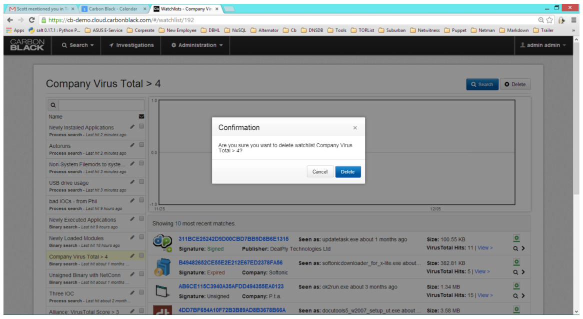


*Figure 10 Test Watchlist*

6. Delete the old Watchlist.

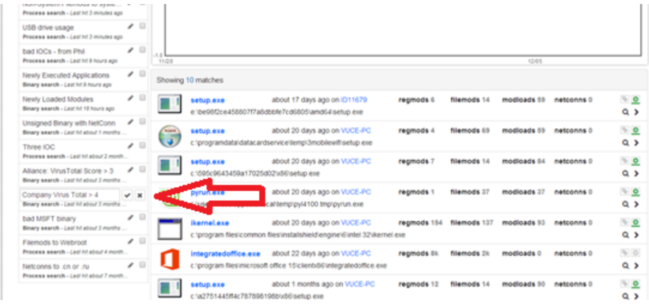

Company Virus Total > 4

Confirmation

Are you sure you want to delete watchlist Company Virus Total > 4?

*Figure 11 Delete Old Watchlist*

7. Edit the name of Temp Watchlist name by selecting the pencil symbol and rename it to the Watchlist deleted in the previous step.



USB drive usage
Process search - Last hit 3 minutes ago
bad IOCs - from Phil
Process search - Last hit 9 hours ago
Newly Executed Applications
Binary search - Last hit 9 hours ago
Newly Loaded Modules
Binary search - Last hit 18 hours ago
Unsigned Binary with NetConn
Binary search - Last hit about 1 months ...
Three IOC
Process search - Last hit about 2 month...
Alliance: VirusTotal Score > 3
Binary search - Last hit about 3 months ...
Company Virus Total > 4
Binary search - Last hit about 3 months ...
bad MSFT binary
Binary search - Last hit about 3 months ...
Filemods to Webroot
Process search - Last hit about 4 month...
Netconns to .cn or .ru
Process search - Last hit about 7 month...

Showing 10 matches

```
setup.exe              about 17 days ago on ID11679   regmods 6    filemods 14   modloads 59  netconns 0
e:\be98f2ce458807f7a6dbbfe7cd6805\amd64\setup.exe
setup.exe              about 20 days ago on VUCE-PC   regmods 4    filemods 69   modloads 59  netconns 0
c:\programdata\datacardservice\temp\3mobilewifi\setup.exe
setup.exe              about 20 days ago on VUCE-PC   regmods 7    filemods 14   modloads 84  netconns 0
c:\595c9643459a17025d02\x86\setup.exe
pyrun.exe              about 20 days ago on VUCE-PC   regmods 1    filemods 37   modloads 37  netconns 0
cal\temp\pyi4100.tmp\pyrun.exe
ikernel.exe            about 20 days ago on VUCE-PC   regmods 154  filemods 137  modloads 93  netconns 0
c:\program files\common files\installshield\engine\6\intel 32\ikernel.exe
integratedoffice.exe   about 22 days ago on VUCE-PC   regmods 8k   filemods 2k   modloads 0   netconns 0
c:\program files\microsoft office 15\clientx86\integratedoffice.exe
setup.exe              about 1 months ago on VUCE-PC  regmods 12   filemods 14   modloads 90  netconns 0
c:\a2751445ff4c787898198b\x86\setup.exe
```

*Figure 12 Rename Watchlist*

## Conclusion

Refining Watchlist entries for your environment will take some time as you expand Carbon Black sensors in the network; however, once refined they are a very effective tool in combating malware.  Caution should be used when ignoring binaries as it may be authorized to run on certain admin computers but not on generic production workstations.  Without the use of advanced conditionals you could ignore malicious activity.