

Configure Custom Detections - Advanced with ClamAV SIGTOOL.EXE on Windows

Contents

[Introduction](#)

[About Advanced Custom Detections](#)

[Why ClamAV](#)

[How to Create Custom Detections - Advanced with sigtool.exe](#)

[Requirements to Save Signature in Secure Endpoint Console](#)

Introduction

This document describes how to create Custom Detections - Advanced using ClamAV sigtool.exe on Windows.

About Advanced Custom Detections

Advanced Custom Detections are like traditional antivirus signatures, but they are written by the user. In order to detect malware and other file-based threats, ClamAV relies on signatures to differentiate clean and malicious/unwanted files. ClamAV signatures are primarily text-based and conform to one of the ClamAV-specific signature formats associated with a given method of detection. These signatures can inspect various aspects of a file and have different signature formats. Some of the available signature formats are:

• MD5 signatures

• MD5, PE section-based signatures

• File body-based signatures

• Extended signature format (offsets, wildcards, regular expressions)

• Logical signatures

• Icon signatures

The ClamAV project distributes a collection of signatures in the form of CVD (ClamAV Virus Database) files. The CVD file format provides a digitally-signed container that encapsulates the signatures and ensures that they cannot be modified by a malicious third-party. This signature set is actively maintained by **Cisco Talos** and can be downloaded using the **freshclam** application that ships with ClamAV.

Why ClamAV

We use ACD to match complex detections/file attributes which is cannot be detected using SHA256 Hashes like those in the examples bellow:

Body-based Signature Content Format

ClamAV stores all body-based (content-based) signatures in a hexadecimal format, with exception to ClamAV YARA rule support. By a hex-signature we mean a fragment of malware's body converted into a hexadecimal string which can be additionally extended using various wildcards.

- **Logical signatures**

Logical signatures allow combining of multiple signatures in extended format using logical operators. They can provide both more detailed and flexible pattern matching.

- **Extended signature format**

The extended signature format is ClamAV most basic type of body-based signature since the deprecation of the original .db database format.

Extended signatures allow for specification of additional information beyond just hexadecimal content such as a file "target type", virus offset, or engine functionality level (FLEVEL), making the detection more reliable

Phishing Signatures

ClamAV can detect HTML links that look suspicious when the display text is a URL that is a different domain than than in the actual URL. Unfortunately, it is pretty common for a company to contract out web services and to use HTML link display text to make it look like it is a link to the company website. Because this practice is commonplace, ClamAV only does phishing checks for specific websites that are popularly targeted by phishing campaigns

Bytecode Signatures

Bytecode Signatures are the means by which more complex matching can be performed by writing C code to parse sample content at various stages in file extraction.

Signatures based on container metadata

ClamAV 0.96 allows creating generic signatures matching files stored inside different container types which meet specific conditions. The signature format is:

```
VirusName:ContainerType:ContainerSize:FileNameREGEX:  
FileSizeInContainer:FileSizeReal:IsEncrypted:FilePos:  
Res1:Res2[:MinFL[:MaxFL]]
```

where the corresponding fields are:

VirusName: Virus name to be displayed when signature matches.

ContainerType: The file type containing the target file. For example:

```
CL_TYPE_ZIP,  
CL_TYPE_RAR,  
CL_TYPE_ARJ,  
CL_TYPE_MSCAB,  
CL_TYPE_7Z,  
CL_TYPE_MAIL,  
CL_TYPE_POSIX_TAR,  
CL_TYPE_OLD_TAR,  
CL_TYPE_CPIO_OLD,  
CL_TYPE_CPIO_ODC,  
CL_TYPE_CPIO_NEWC,  
CL_TYPE_CPIO_CRC  
and so on.
```

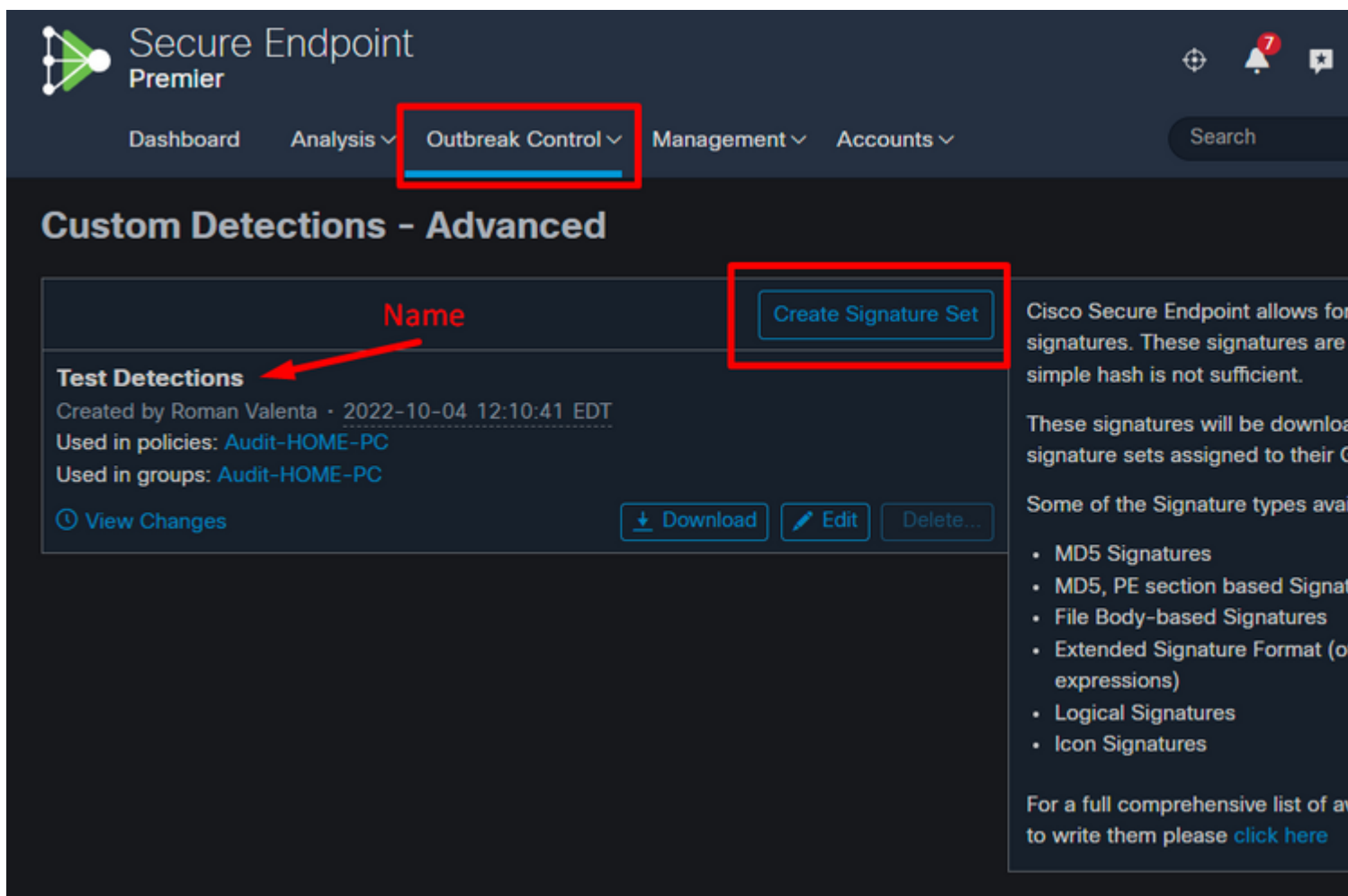
This document is focusing on hash signatures.

Note: The easiest way to create signatures for ClamAV is to use filehash checksums, however this method can be only used against static malware.

Caution: Please note that information in this document are subject to change with newer releases of ClamAV. Always correlate and verify with [official guide](#) for ClamAV.

More information on signature formats can be found at: [ClamAV Website](#)

These signatures are compiled into a file that is downloaded to the endpoint. In order to create advanced custom detections, go to **Outbreak Control > Advanced**. Click **Create Signature Set** to create a new Advanced Custom Detection set, give it a name, and click Create.



â€f

After you create the Advanced Custom Detection set, click Edit and you can see the **Add Signature** link. Enter the name of your signature and click Create.

Custom Detections - Advanced

Create Signature Set

Test Detections
Created by Roman Valenta · 2022-10-04 12:10:41 EDT
Used in policies: [Audit-HOME-PC](#)
Used in groups: [Audit-HOME-PC](#)
[View Changes](#) [Download](#) [Edit](#) [Delete...](#)

Test Detections
Created by Roman Valenta · 2
[Add Signature](#) [Build Database](#)
hdb: TestVirusRV.exe.UNOFFIC

â€f

After all of your signatures are listed, select **Build a Database from Signature Set**. If you accidentally add a signature you did not want, you can delete it by clicking Remove.

Warning: Any time you add or remove a signature you **MUST** click on Build a Database from Signature Set

Note: When you create an advanced custom detection for a file, it is subject to caching for an hour. If a file is added to an advanced custom detection set, the cache time must expire before the detection takes effect. For example, if you add an advanced custom detection for an unknown file 5 minutes after it was cached, the detection is not going to take effect for another 55 minutes.

Warning: Advanced Custom Detections only work on files of unknown disposition.

How to Create Custom Detections - Advanced with sigtool.exe

Step 1: First we need to obtain the sigtool by navigation to the ClamAV website [downloads](#)

In my case I download the ZIP package **clamav-1.1.0.win.x64.zip**

Download

Download the official source code using the links below. We recommend running the latest stable release or the latest Long Term Support release on production systems. [Click here](#) learn more about ClamAV. For instructions on how to install third-party Linux and Unix distribution packages, [click here](#).

1.1.0 Latest

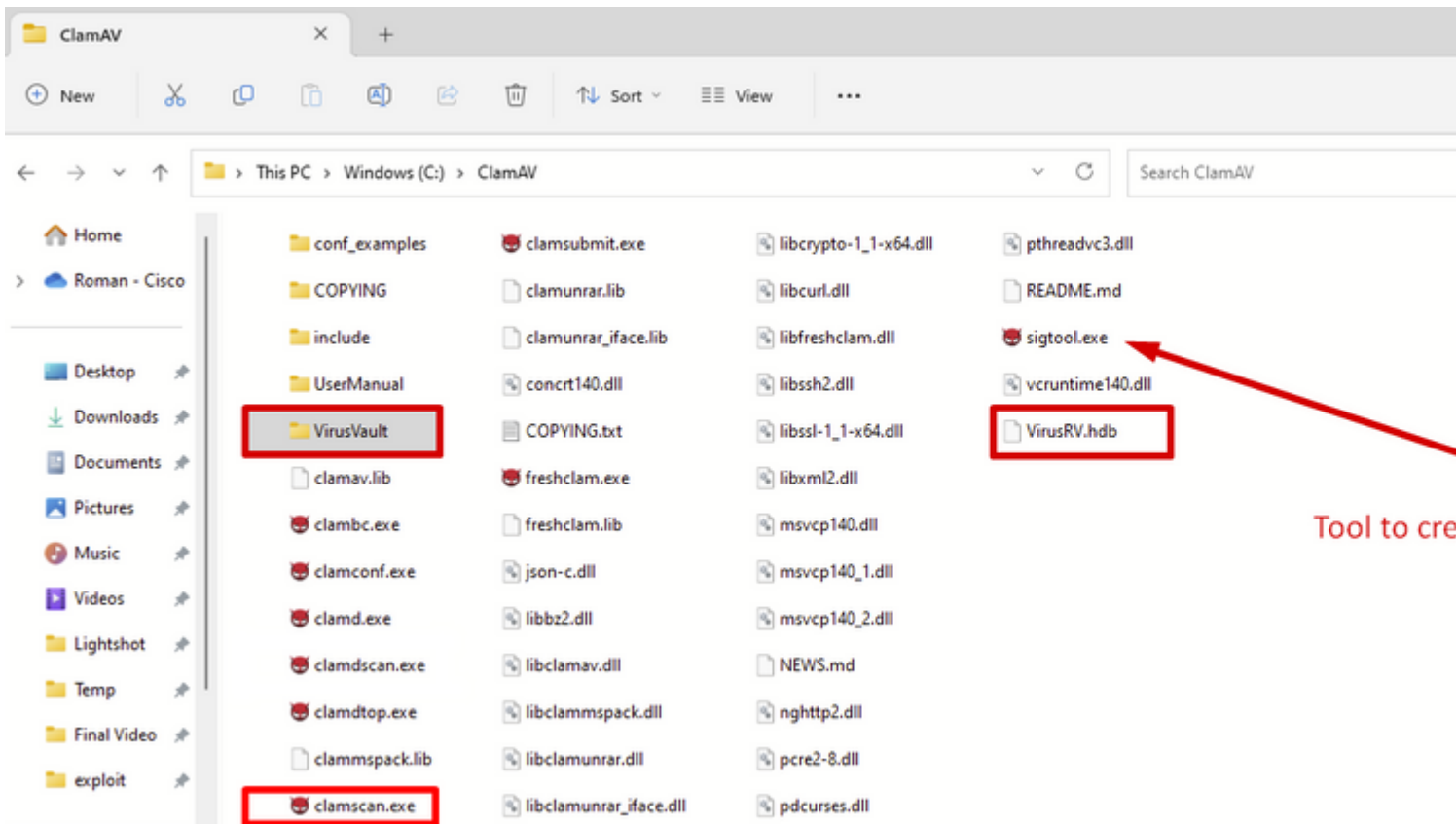
Windows

ClamAV downloads for Windows

file	Modified	Size
clamav-1.1.0.win.win32.zip	2023-05-01 17:08:49 UTC	10.6 MB
clamav-1.1.0.win.x64.msi	2023-05-01 17:08:18 UTC	15.4 MB
clamav-1.1.0.win.x64.zip	2023-05-01 17:07:42 UTC	15.0 MB
clamav-1.1.0.win.win32.msi	2023-05-01 17:09:23 UTC	11.0 MB
clamav-1.1.0.win.x64.msi.sig	2023-05-01 17:02:23 UTC	801 bytes
clamav-1.1.0.win.win32.msi.sig	2023-05-01 17:03:28 UTC	801 bytes
clamav-1.1.0.win.x64.zip.sig	2023-05-01 17:02:28 UTC	801 bytes
clamav-1.1.0.win.win32.zip.sig	2023-05-01 17:02:16 UTC	801 bytes

â€š

Step 2: Unzip the file in to preferred location. In my case I used C:/ClamAV



â€š

â€f

Please note highlighted folders and files.

clamscan.exe â€“ is a command line tool which is used to scan files and/or directories for viruses. Unlike clamscan, clamscan does not require a running clamd instance to function. Instead, clamscan create a new engine and load in the virus database each time it is run. It going to scan the files and/or directories specified at the command line, create a scan report, and exit.

sigtool.exe â€“ Tool that creates and format signature and write in to *.hdb file. The hdb extension refers to Hash-based Signatures. sigtool pulls in libclamav and provides shortcuts to doing tasks that clamscan does behind the scenes. These can be really useful when writing a signature or trying to get information about a signature that can be causing FPs or performance problems.

VirusVault â€“This is my own folder that was created to drop files for which I wanted to create custom signature.

VirusRV.hdb â€“ This file contains formatted signatures. I named this file VirusRV but you can use any meaningful name.

Step 3a: Launch CMD line and navigate to the location where you previously unzip your ClamAV.

â€f

```
Microsoft Windows [Version 10.0.22621.1848]
(c) Microsoft Corporation. All rights reserved.

C:\Users\rvalenta>cd C:\ClamAV
```

Step 3b Execute this line.

```
C:\ClamAV>sigtool --md5 location-of-the-custom-file > name-of-the-output-file.hdb
```

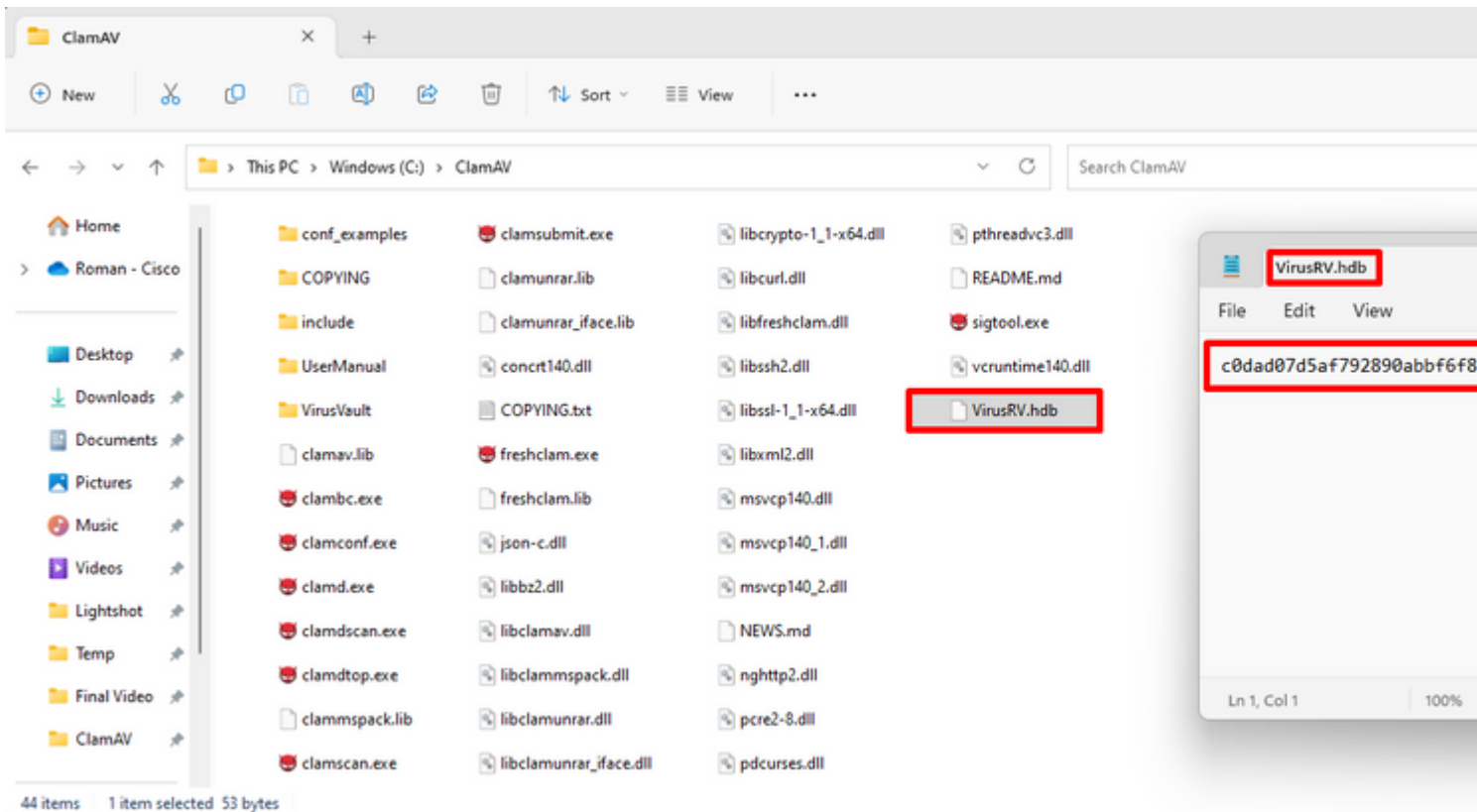
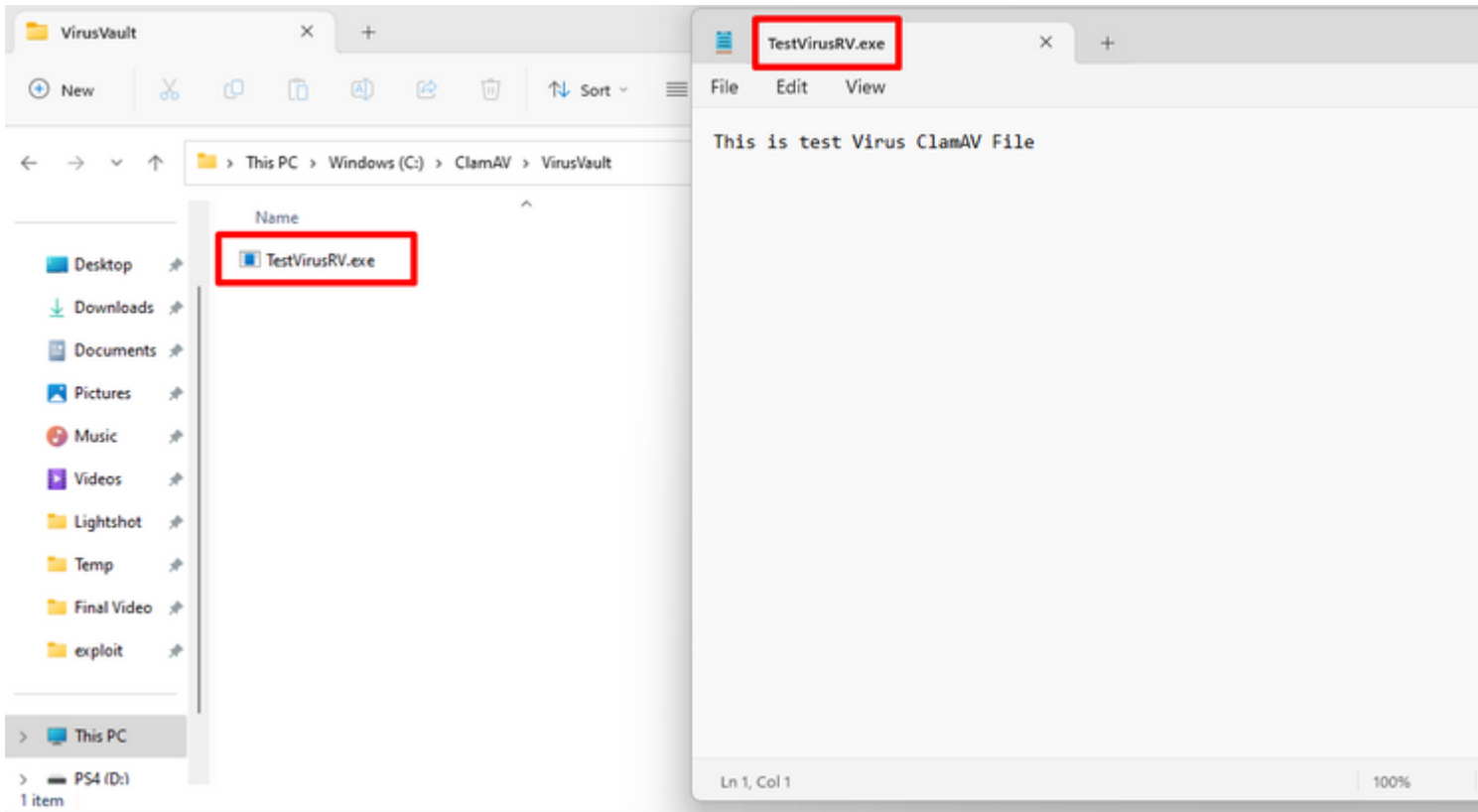
You can change the name (by default sigtool uses the name of the file) and place it inside a *.hdb file. A single database file can include any number of signatures. To get them automatically loaded each time clamscan/clamd starts just copy the database file(s) into the local virus database directory (eg. /usr/local/share/clamav).

```
C:\ClamAV>sigtool --md5 C:\ClamAV\VirusVault\TestVirusRV.exe > VirusRV.hdb
```

```
C:\ClamAV>sigtool --md5 C:\ClamAV\VirusVault\TestVirusRV.
```

This creates the signature in this case for the file named **TestVirusRV.exe** and then write the signature to file named **VirusRV.hdb**

â€f



Note: If you like to create signature based on SHA value the corresponding file is then saved as *.hsb

```
C:\ClamAV>sigtool --md5 C:\ClamAV\VirusVault\TestVirusRV.exe > VirusRVsha256.hsb
```

Custom Detections - Advanced

Test Detections
Created by Roman Valenta · 2022-10-04 12:10:41 EDT
Used in policies: [Audit-HOME-PC](#)
Used in groups: [Audit-HOME-PC](#)
[View Changes](#) [Download](#) [Edit](#) [Delete...](#)

Test Detections
Created by Roman Valenta ·
[Add Signature](#) [Build Data](#)
hsb: TestVirusRV1.exe.UNO
Signature contents:
4345167de05e6621add5af
62f9d8bbd82:30:TestVirusR
hdb: TestVirusRV.exe.UNO

SHA256

Caution: The hash-based signatures shall not be used for text files, HTML and any other data that gets internally preprocessed before pattern matching. If you really want to use a hash signature in such a case, run clamscan with `--debug` and `--leave-temps` and create a signature for a preprocessed file left in `/tmp`. Please keep in mind that a hash signature going to stop matching as soon as a single byte changes in the target file. More can be found [here](#)

These sigtool flags can be especially useful for signature writing:

`--md5 / --sha1 / --sha256`: Generate the MD5/SHA1/SHA256 hash and calculate the file size, outputting both as a properly-formatted `.hdb/.hsb` signature

Signature names

ClamAV signatures must only use alphanumeric characters, dash (-), dot (.), underscores (_) to delimit words. Never use a space, apostrophe, colon, semi-colon, or quote mark.

ClamAV signature names found in the official signature databases generally use this format:

```
{platform}.{category}.{name}-{signature id}-{revision}
```


Naming conventions in 3rd party databases vary. You can find Cisco-Talos guidelines for naming signatures for the official database [here](#).

Tip: If you want to create multiple signatures on files located in the directory that you created earlier in my case I named mine VirusVault you can run the command using wild card. In this case I ran mine as:


```
C:\ClamAV>sigtool --md5 C:\ClamAV\VirusVault\wildcard\ > VirusRV.hdb
```

```
C:\ClamAV>sigtool --md5 C:\ClamAV\VirusVault\*\ > VirusRV.hdb
```

```
C:\ClamAV>  
C:\ClamAV>  
C:\ClamAV>  
C:\ClamAV>sigtool --md5 C:\ClamAV\VirusVault\*\ > VirusRV.hdb
```



â€f

Which created signature against each file located in the directory **VirusVault**

Step 4: Verify the signature by running this command.

```
C:\ClamAV>clamscan -d VirusRV.hdb C:\ClamAV\VirusVault\TestVirusRV.exe
```

```
C:\ClamAV>clamscan -d VirusRV.hdb C:\ClamAV\VirusVault\Te  
Loading:      0s, ETA:      0s [=====>]  
Compiling:    0s, ETA:      0s [=====>]  
  
C:\ClamAV\VirusVault\TestVirusRV.exe: TestVirusRV.exe.UNC  
  
----- SCAN SUMMARY -----  
Known viruses: 1  
Engine version: 1.1.0  
Scanned directories: 0  
Scanned files: 1  
Infected files: 1  
Data scanned: 0.00 MB  
Data read: 0.00 MB (ratio 0.00:1)  
Time: 0.021 sec (0 m 0 s)  
Start Date: 2023:06:26 19:02:53  
End Date: 2023:06:26 19:02:53
```

To verify all signatures you can again use wild card mask.

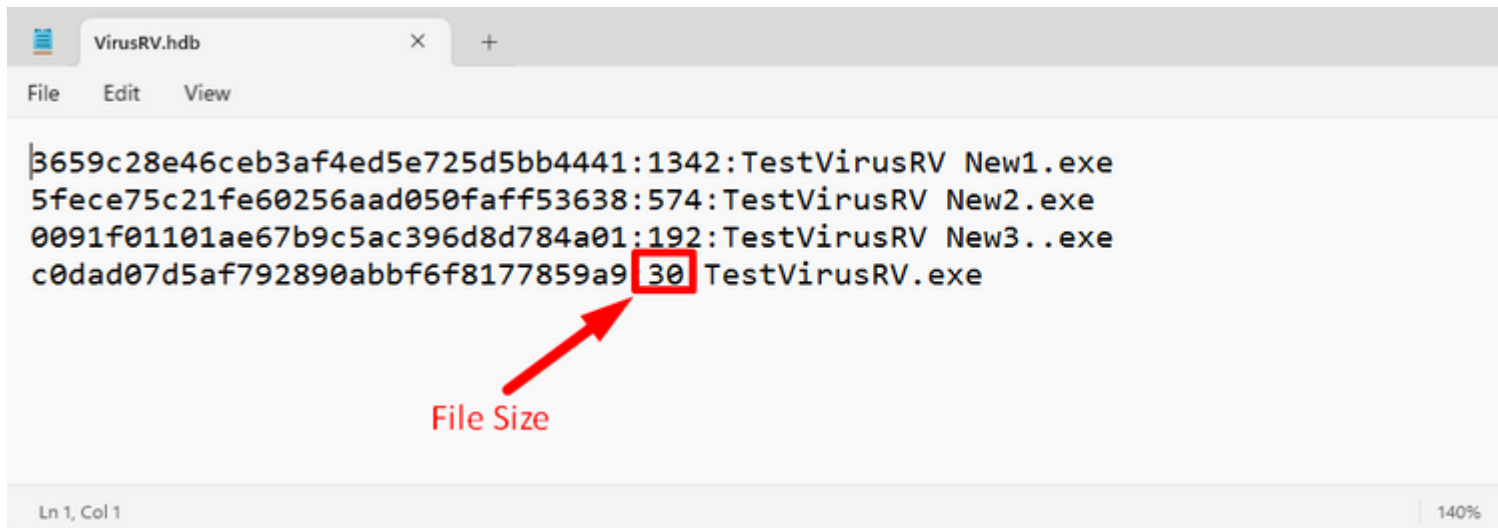
```
C:\ClamAV>clamscan -d VirusRV.hdb C:\ClamAV\VirusVault\*\
```

```
C:\ClamAV>clamscan -d VirusRV.hdb C:\ClamAV\VirusVault\*\
Loading:      0s, ETA:  0s [=====>]           4/4 si
Compiling:    0s, ETA:  0s [=====>]           10/10 t

C:\ClamAV\VirusVault\TestVirusRV New1.exe: TestVirusRV New1.exe.UNOFFI
C:\ClamAV\VirusVault\TestVirusRV New2.exe: TestVirusRV New2.exe.UNOFFI
C:\ClamAV\VirusVault\TestVirusRV New3..exe: TestVirusRV New3..exe.UNO
C:\ClamAV\VirusVault\TestVirusRV.exe: TestVirusRV.exe.UNOFFICIAL FOUR

----- SCAN SUMMARY -----
Known viruses: 4
Engine version: 1.1.0
Scanned directories: 0
Scanned files: 4
Infected files: 4
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 0.024 sec (0 m 0 s)
Start Date: 2023:06:27 07:40:55
End Date: 2023:06:27 07:40:55
```

â€f



```
VirusRV.hdb
File Edit View

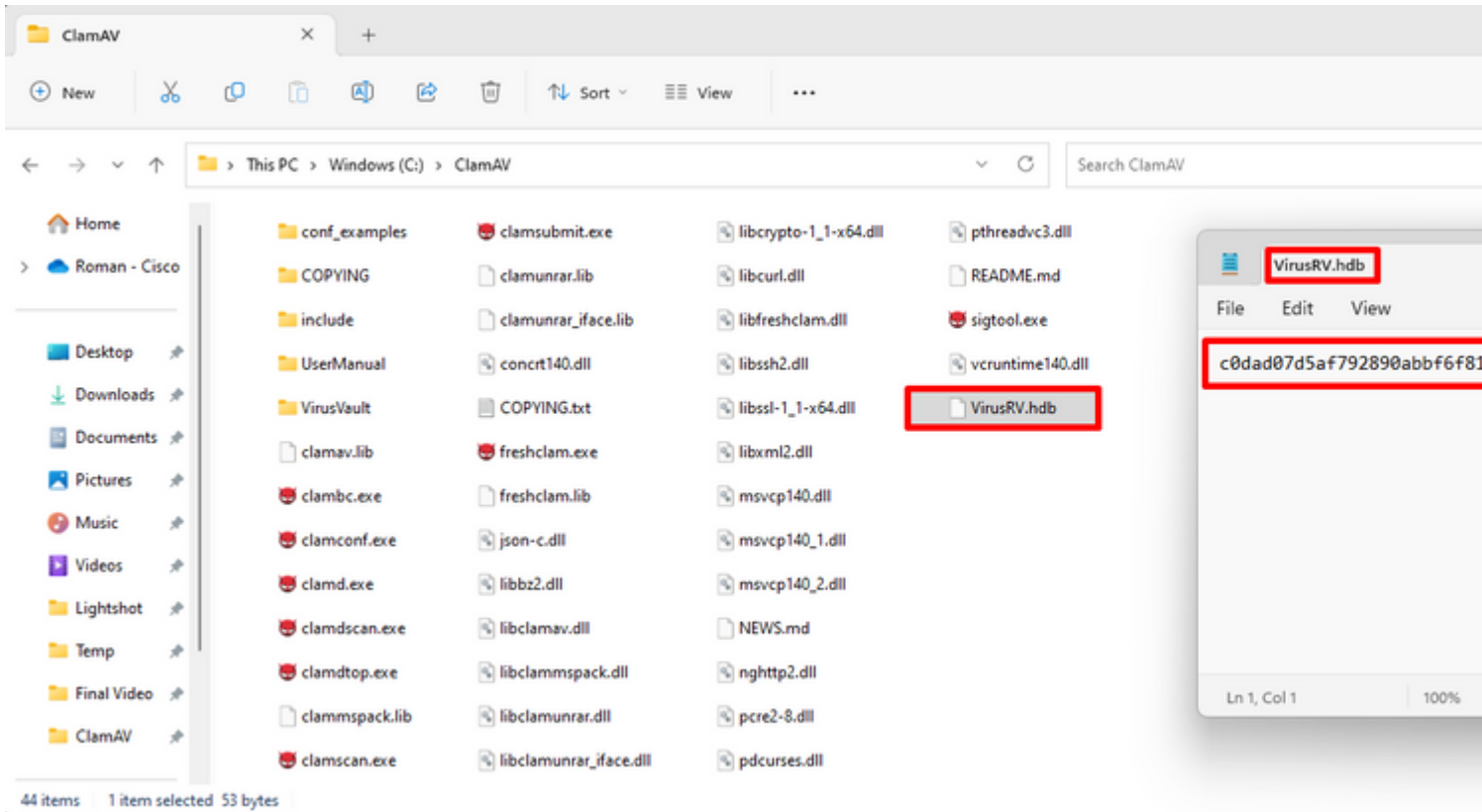
|3659c28e46ceb3af4ed5e725d5bb4441:1342:TestVirusRV New1.exe
5fece75c21fe60256aad050faff53638:574:TestVirusRV New2.exe
0091f011101ae67b9c5ac396d8d784a01:192:TestVirusRV New3..exe
c0dad07d5af792890abbf6f8177859a9|30| TestVirusRV.exe

Ln 1, Col 1 140%
```

â€f

â€f

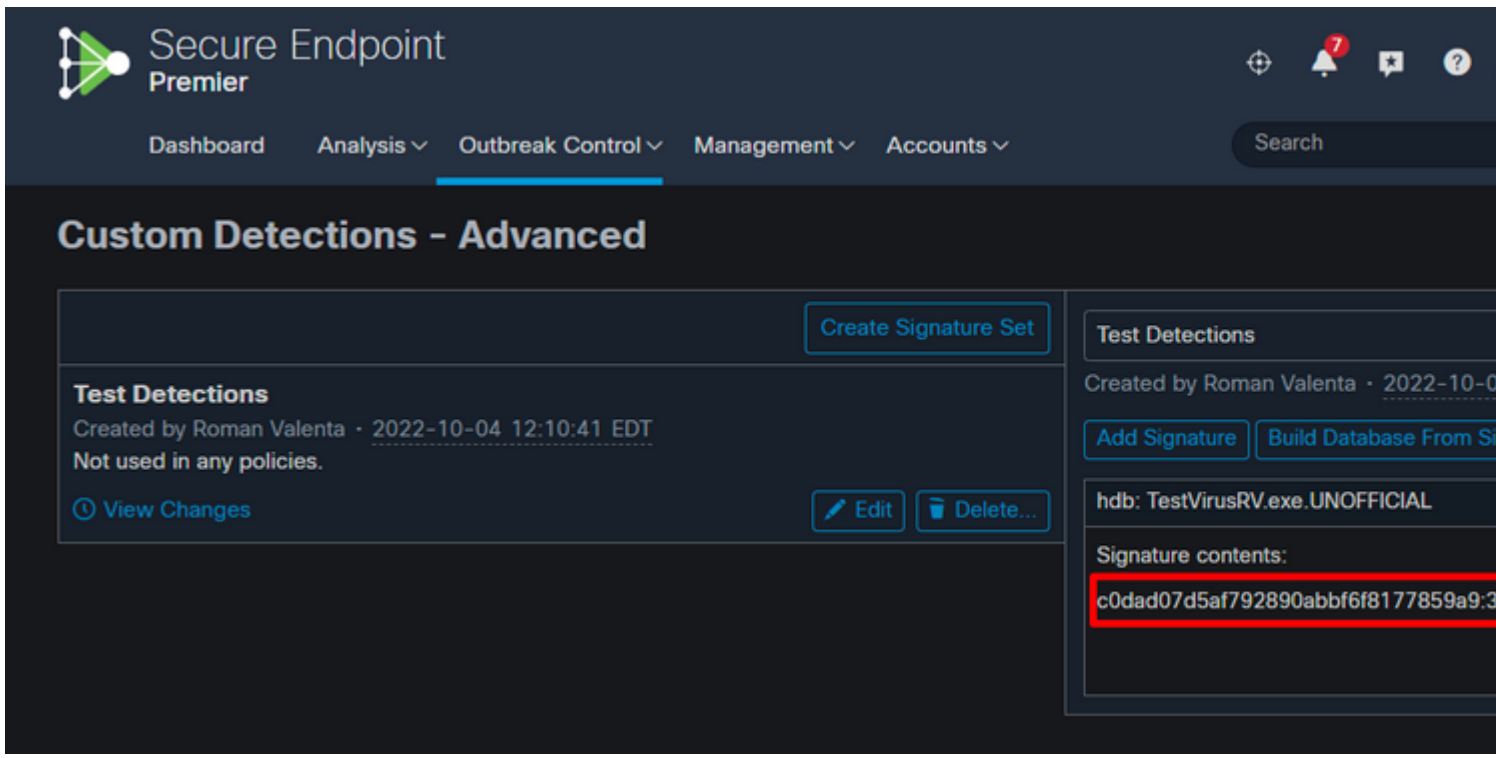
Step 5: Open newly created *.hdb file and copy created signature and then navigate to your secure endpoint console under **Outbreak Control > Advanced** click Edit and you can see the **Add Signature** link.



â€f

â€f

â€f



Step 6: Make sure you click on Build a Database from Signature Set then apply the new Custom Detections to your policy.

< Edit Policy

Windows

Name Audit-HOME-PC

Description This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantine them. Malicious network traffic is also detected

Modes and Engines

Exclusions
22 exclusion sets

Proxy

Outbreak Control

Device Control

Product Updates

Advanced Settings

Custom Detections - Simple

Simple Custom Detection List

Custom Detections - Advanced

Test Detections

Application Control - Allowed

Allowed Application List

Application Control - Blocked

Blocked Application List

Network - IP Block & Allow Lists

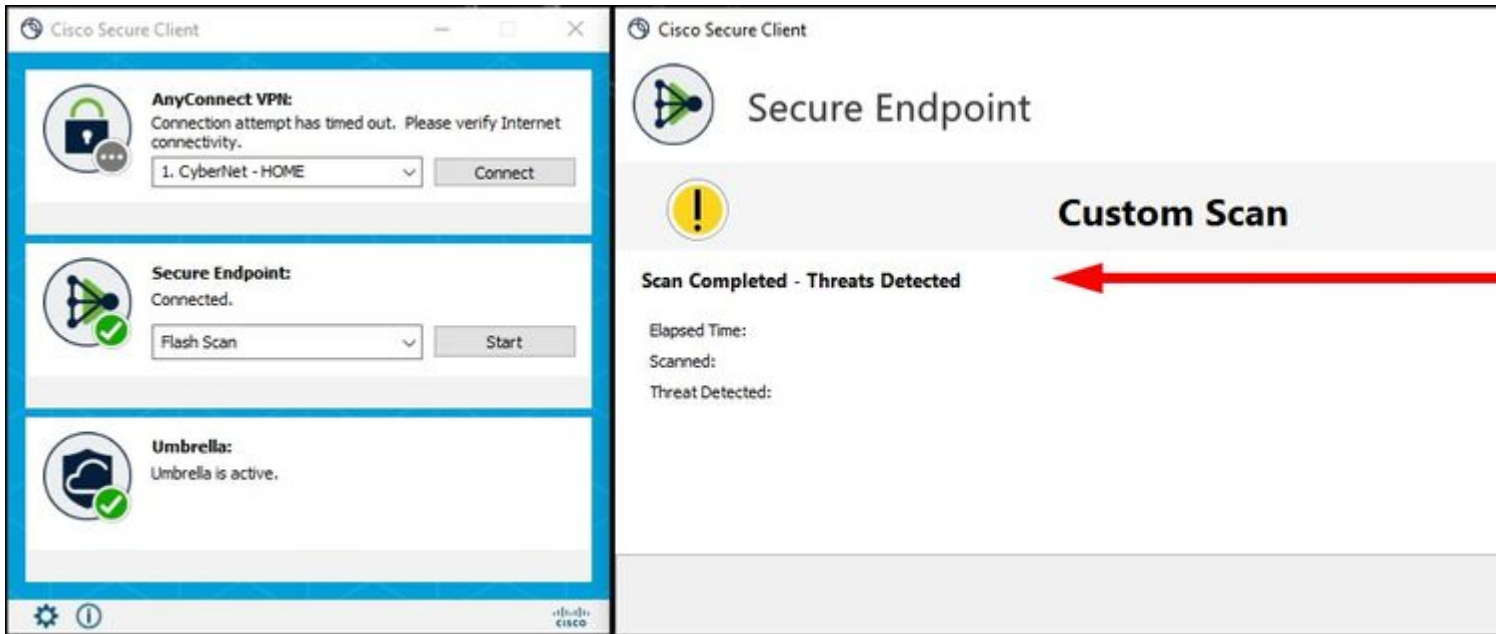
None

Clear Select Lists

â€f

Step 7: Sync up your policy on your endpoint and test your new signature with manual scan. You can see results like those listed below.

Manual Scan



Detections in Secure Endpoint Console



Dashboard

Dashboard **Inbox** Overview Events IOS Clarity

Refresh All

Auto-Refresh



Reset

New Filter

30 days

20

4.8%

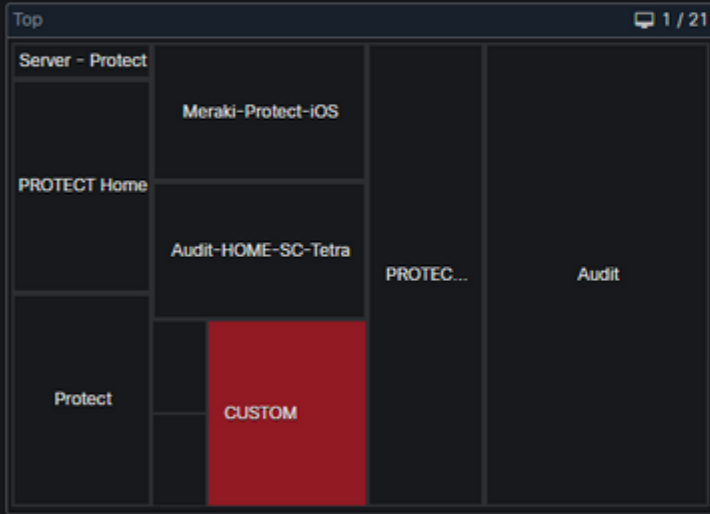
compromised

Inbox Status

1 Requires Attention 0 In Progress 0 Resolved

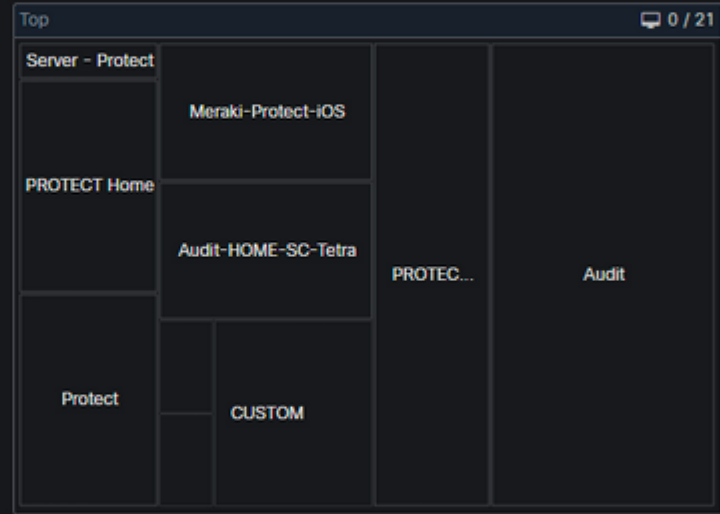
Compromises

Inbox



Quarantined Detections

Quarantine Events



27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
MAY JUN

27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
MAY JUN

Significant Compromise Observables

FILE	4345167d...9d8bbd82	TestVirusRV.exe	1
------	---------------------	-----------------	---

Compromise Event Types

Medium	Threat Detected	1
Medium	Scan Completed With Detections	1

â€f

Event Expanded

â€f

VMStation-1 Scanned 1 files, 0 processes, 0 directories. Found 1 malicious items. Medium

Connector Details	Computer	VMStation-1
Comments	Connector GUID	c4e1b294-476e-4294-82e5-f306a50b1ea9
	Cisco Secure Client ID	72895c3b-ec19-4a7e-904f-3f905a2a9052
	Processor ID	bfebfbff000406e3
	Current User	None
	Run Scan	

VMStation-1 detected TestVirusRV.exe as Clam.TestVirusRV.exe.UNOFFICIAL Tactics Medium

File Detection	Detection	Clam.TestVirusRV.exe.UNOFFICIAL			
Connector Details	MITRE ATT&CK	Tactics	TA0002: Execution TA0011: Command and Control TA0042: Resource Development		
		Techniques	T1105: Ingress Tool Transfer T1204: User Execution T1204.003: User Execution: Malicious I		
Comments	Fingerprint (SHA-256)	4345167d...9d8bbd82			
	File Name	TestVirusRV.exe			
	File Path	C:\Users\User\Downloads\TestVirusRV.exe			
	File Size	30 B			
	Parent	No parent SHA/Filename available.			
	Analyze		View Upload Sta		

Requirements to Save Signature in Secure Endpoint Console

If you only have MD5 hash and you don't know the size of the file you can still create signature set but you must use these rules:

A: MD5 cannot contain all uppercase letters

Correct MD5 Hash:

5b852928a129d63dc5c895bd62cf2ab7

Incorrect MD5 Hash:

5B852928A129D63DC5C895BD62CF2AB7

Error in Secure Endpoint Console with ALL upper case letters

Custom Detections - Advanced

Create Signature Set

Test Detections

Created by Roman Valenta · 2022-10-04 12:10:41 EDT

Used in policies: [Audit-HOME-PC](#)

Used in groups: [Audit-HOME-PC](#)

[View Changes](#)

[Download](#)

[Edit](#)

[Delete...](#)

Test Detections

Created by Roman Valenta

[Add Signature](#)

[Build Data](#)

Add Signature

3 errors prohibited
taking place

- Content sign
find virusnan
- Content Unk
- Content synt
cli_load: unk
/tmp/signalic
signature ignr

Signature

Type [Auto detect](#)

See [Signature Format Do](#)
documentation, or choos
documentation and overv

hdb: TestVirusRV.exe.UNO

â€f

B: You must use upper case letter for naming and it could be your own name.

Correct Name:

Dm-launcher.msi

Incorrect Name:

dm-launcher.msi

C: You can use wild card for the size but you must use :73 for minimum FLEVEL

Correct Wild Card:

5b852928a129d63dc5c895bd62cf2ab7:*:dm-launcher.msi:73

Incorrect Wild Card:

5b852928a129d63dc5c895bd62cf2ab7*:dm-launcher.msi

Error in Secure Endpoint Console for all lower case name and no FLEVEL specified

Note: Hash signatures with unknown size - ClamAV 0.98 has also added support for hash signatures where the size is not known but the hash is. It is much more performance-efficient to use signatures with specific sizes, so be cautious when using this feature. For these cases, the $\hat{\epsilon}^{\text{TM}}*\hat{\epsilon}^{\text{TM}}$ character can be used in the size field. To ensure proper backwards compatibility with older versions of ClamAV, these signatures must have a minimum functional level of 73 or higher. Signatures that use the wildcard size without this level set is rejected as malformed.

Custom Detections - Advanced

Create Signature Set

Test Detections

Created by Roman Valenta · 2022-10-04 12:10:41 EDT

Used in policies: [Audit-HOME-PC](#)

Used in groups: [Audit-HOME-PC](#)

[View Changes](#)

[Download](#)

[Edit](#)

[Delete...](#)

Test Detections

Created by Roman Valenta · 2022-10-04 12:10:41 EDT

[Add Signature](#)

[Build Database](#)

Add Signature

2 errors prohibited taking place

- Content virusname: capital letter: d launcher.msi.UNOFFICIAL
- Content syntax: cli_loadhash: M must be at least 73 for signatures. For example: is 129 LibClamAV Error: Problem parsing signature: /tmp/sigvalidate/z6c2bf.hdb: Malformed failed: Malformed

Signature

Type [Auto detect](#)

See [Signature Format Documentation](#) for more documentation, or choose a [signature type](#) for more documentation and overview

hdb: TestVirusRV.exe.UNOFFICIAL