VIRUSTOTAL TIPS, TRICKS AND MYTHS

Randy Abrams
Independent security analyst, USA

Email randyab@comcast.net

ABSTRACT

Outside of the anti-malware industry, users of *VirusTotal* users generally believe it is simply a virus-scanning service. Most users quickly reach erroneous conclusions about the meaning of various scanning results. At the same time, many very technical people are unaware that *VirusTotal* provides a wealth of contextual and forensic information. Most people do not realize that *VirusTotal* is a multi-directional threat intelligence feed as well.

After a brief introduction to the history of *VirusTotal* and its role in today's security ecosystem, the myths listed below will be debunked, and little-known features of *VirusTotal* will be demonstrated.

- Myth 1: *VirusTotal* can be used to perform comparative testing.
- Myth 2: Detection of malware on *VirusTotal* means the scanner has detection of the malware.
- Myth 3: Lack of detection on *VirusTotal* means the file is safe.
- Myth 4: Lack of detection on *VirusTotal* means the scanner doesn't detect it.
- Myth 5: False positive means false positive.
- Myth 6: More is better.
- Myth 7: Malicious website means malicious website.

Information that can be obtained using the tabs for 'File Details', 'Relationships', 'Additional Information', 'Comments', and 'Votes' will be reviewed. Some additional resources available to users will be touched on, and the need to read the terms of service will be emphasized.

Disclaimer: The most pedantic readers of this paper will at times take issue with me saying 'anti-virus' instead of 'anti-malware', and 'virus scanner' instead of 'malware scanner'. With the exception of the discussion of specific types of malware, the terms 'virus' and 'malware' are synonymous for most people. The battle for differentiation was lost more than a billion malware samples ago. *Symantec* (*Norton*), *McAfee*, *Trend Micro*, *ESET*, *Kaspersky*, *Bitdefender*, and many others include the word 'Antivirus' in the names of their products.

REM That's enough to prove my point.[1]

VirusTotal was launched in June 2004 by the Spanish security company *Hispasec*. In June 2012 *VirusTotal* was acquired by *Google*. Today, *VirusTotal* is a wholly owned subsidiary of *Google*. Initially, *VirusTotal* began as a web-based virus-scanning service utilizing a handful of virus scanners. *VirusTotal* has since grown to include dozens of scanners, threat analysis and other contextual threat intelligence.

VirusTotal is widely known as a virus-scanning service and it is true that *VirusTotal* will run a file through a battery of anti-malware products. However, many people – including IT professionals – do not know that *VirusTotal* accepts input such as IP addresses and domains, or that much more information is available besides the results of a scan.

GETTING SAMPLES TO VIRUSTOTAL

There are multiple ways to submit files, URLs, etc. for scanning. The method that most people are familiar with is using the landing page at www.virustotal.com. Files, file hashes, URLs, domain names and IP addresses can all be submitted.

- If there is no particular urgency, files can be sent via email. Email submissions have the lowest priority for scanning of all of the other methods [1].
- *VTZilla* is a *Firefox* extension that facilitates the scanning of files and URLs via the right-click context menu on links and the download dialog box. Links in emails can also be submitted to *VirusTotal* for phishing [2].
- The *VirusTotal Windows* uploader adds a context menu item to *Windows Explorer.* Files can also be dragged and dropped onto a desktop icon and there is command-line functionality [3].
- *VirusTotal* has an *Android* application that will provide scan results of apps on the device. As *VirusTotal* notes, the *VirusTotal* app does not provide protection, it is simply for reporting. *VirusTotal* will not prevent a threat from getting onto the system, and it will not remove malicious apps [4].
- There are public and private APIs. The public API is free and provides more information than the average user even knows is present on *VirusTotal*. To get started it is a requirement that you sign up to the *VirusTotal* community. *VirusTotal* does not spam people and the community shares a lot of information.

  Upon signing up you will obtain a free key that is required to use the API. The documentation for the API includes code samples and can be found at [5]. The frequency of submissions allowed using the public API is limited, but is probably more than adequate for most users, as is the richness of information returned.

  The private API is well known to security companies and to most IT professional that utilize threat feeds. The private API allows for a higher rate of submissions, but also adds the ability to retrieve significantly more information from *VirusTotal*. More information about the private API can be found at [6] and [7].

Submitting files, etc. is the easy part. It is when the results are returned that *VirusTotal* mythology kicks in. *VirusTotal* is Zeus and each virus scanner is a lesser deity. The lesser deities often appear to disagree with each other, even when they do agree on something.

I AM CONFUSED ALREADY

The genesis of a myth frequently lies in the oral tradition of an incorrect, or partially correct explanation of something that is

[1] A reference to the Concept macro virus which displayed a dialog box containing the text '1'. Inside the macro was a remarked line reading 'That's enough to prove my point'.

misunderstood to begin with. At some point the myth is transcribed so that it can be cited as fact – as some may claim is the case with this paper. For the average user who simply wants to know if a file is safe, results such as PUP, PUA, potentially dangerous application, etc. can be quite confusing. In some cases detection reports will indicate PUPs, PUAs, riskware, trojans, and more for the same sample. These classifications may lead to confusion as to whether or not their scanner is protecting them.

Consider this riddle: If he is she, then who is he, and is a dog a fish? The answer will be provided in due course.

THE RABBIT OF CAERBANNOG – 'WELL, THAT'S NO ORDINARY RABBIT!'[2]

Many years ago, an email containing a file claiming to be about a cute or funny bunny rabbit was circulated. The subject line and message body indicated the attached item would display a bunny rabbit and have audio that must be listened to. Upon engaging in the deadly 'double-click of death', a dialog box saying 'GOTCHA. HAVE A NICE DAY' would be displayed and a voice from the computer would yell 'Hey everybody I'm watching porno over here, woo hoo!'

Figure 1: Not a bunny rabbit.

Perhaps you remember the NiceDay macro virus. This is not the NiceDay macro virus.

Let's run rabbit.exe through *VirusTotal* and see what the results are.

The results include seven detections of Gen:Variant.Zusy.Elzob.14268 and two other miscellaneous versions of Zusy (Figure 2). A search for Zusy.Elzob.14268 returns many Zusy Elzobs, but none are the 14268 variant. Most of the descriptions of Zusy Elzobs indicate that these are trojan downloaders, password stealers, and other not so nice applications. The results returned from *VirusTotal* include indications of potential bots, downloaders, and other quite nasty types

[2] A reference to *Monty Python and the Holy Grail*.

virustotal

SHA256: 94abfbb7f96ba8f67f92a99b009771f46e3d63047a8c5a34d315c6eb98ee3a41

File name: 94abfbb7f96ba8f67f92a99b009771f46e3d63047a8c5a34d315c6eb98ee3a41

Detection ratio: 38 / 61

Analysis date: 2017-06-01 04:11:46 UTC (1 week ago)

Analysis | File detail | Relationships | Additional information | Comments 1 | Votes

Antivirus	Result	Update
Ad-Aware	Gen:Variant.Zusy.Elzob.14268	20170601
AegisLab	Gen.Variant.Zusy!c	20170601
ALYac	Gen:Variant.Zusy.Elzob.14268	20170601
Antiy-AVL	Trojan/Win32.Tgenic	20170601
Arcabit	Trojan.Zusy.Elzob.D37BC	20170601
Avast	Win32:PUP-gen [PUP]	20170601
AVG	RabbitJoke	20170601
AVware	Trojan.Win32.GenericIBT	20170601
BitDefender	Gen:Variant.Zusy.Elzob.14268	20170601
ClamAV	Win.Trojan.Joke-41	20170601
Comodo	UnclassifiedMalware	20170601
Cyren	W32/Joke.XLUW-6389	20170601
Emsisoft	Gen:Variant.Zusy.Elzob.14268 (B)	20170601
F-Prot	W32/Joke!03ba	20170601
F-Secure	Gen:Variant.Zusy.Elzob.14268	20170601
Fortinet	Riskware/Rabbit	20170601
GData	Gen:Variant.Zusy.Elzob.14268	20170601
Ikarus	Joke.Win32.Rattib	20170531
K7AntiVirus	Riskware (0040eff71)	20170531
K7GW	Riskware (0040eff71)	20170531
Kingsoft	Win32.Troj.Agent.xb.(kcloud)	20170601
McAfee	Artemis!E88B23DD3445	20170601
McAfee-GW-Edition	Joke-Rabbit	20170601
Microsoft	Joke:Win32/Rattib.B	20170601
eScan	Gen:Variant.Zusy.Elzob.14268	20170601
NANO-Antivirus	Riskware.Win32.03ba.bjmao	20170601
nProtect	Trojan/W32.Agent.315392.BR	20170601
Panda	Generic Malware	20170531
Qihoo-360	Win32/Trojan.8be	20170601
Rising	Trojan.Generic (cloud:8oyVq9ez10G)	20170601
Sophos	Joke/Rabbit	20170601
Symantec	Joke.AnnoyGreet	20170531
TrendMicro	JOKE_RABBIT	20170601
TrendMicro-HouseCall	JOKE_RABBIT	20170601
VIPRE	Trojan.Win32.GenericIBT	20170601
Webroot	Joke:Win32/Rattib.A	20170601
Yandex	Trojan.Agent!N351OD5M0Ig	20170531
Zillya	Trojan.Agent.Win32.184745	20170531

Figure 2: Results of running rabbit.exe through VirusTotal.

of malware. Nine out of 36 indications are for a Zusy of some sort. Six of 36 indicate a generic trojan of some sort. There are indications of unclassified malware, riskware, a PUP, and Artemis!E88B23DD3445. Of note, 12 of the results include the word 'Joke' in the description. Finally, 20 of 36 scanners display no detection. So, who is right?

The answer lies in the riddle 'If he is she, then who is he, and is a dog a fish?'

The English word 'she' is pronounced 'he' in Hebrew. The English word 'he' is pronounced 'who' in Hebrew. Finally, the English word 'dog' (pronounced daag) is the Hebrew word for fish.

The scanners are speaking different languages, some saying the same thing and some saying different things, and so the meaning of the scan results is quite confusing. If he is she and who is he, then we are probably speaking Hebrew and indeed a dog is a fish. But if we are not speaking Hebrew, then a dog is probably not a fish. Let's try a couple of sentences that may or may not have Hebrew words interspersed with English words.

I was out walking my dog in the snow when I ran into a friend of mine. He was wearing a bikini. I always knew he was strange.

Did I say I was walking a fish in the snow and I saw a guy wearing a bikini, or did I say I was walking a member of the canine family in the snow and I saw a girl wearing a bikini?

You can't tell from the results of the scan of rabbit.exe whether you are looking at a program that is a joke, or if the program is malicious. The Rabbit application only made noise and displayed a message box. It would be understandable if one were to assume this application was intended to induce laughter, and perhaps cause a little embarrassment.

Choosing not to detect rabbit.exe is a valid strategy. Choosing to detect rabbit.exe is also valid unless the detection actually is a false positive. Because of the ambiguity and subjectivity of the designation of trojan, PUP, PUA, PDA, etc., it is perfectly valid to detect rabbit.exe.

Consider the following real-world scenario:

An employee in a call centre opened the rabbit.exe attachment. The sound of someone in a cubicle yelling 'Hey everybody I'm watching porno over here, woo hoo!' was heard across the floor. Indeed it was riskware, and/or a PUP, and/or a PUA, and/or a trojan, and/or an inappropriate joke in that situation. I would guess that the employee who sent the email realized the risk when he was fired. Depending on the company, the customers who heard it may have thought 'that explains the lack of customer service'. Choosing not to detect the file can be justified as well. When I first encountered the file I laughed – I still do. To me, it was a joke.

Because neither detection nor non-detection is wrong, the file is not valid as a part of a comparative test. It is possible that a product did generate a false positive, but since the file cannot be used in a comparative test it is irrelevant. A competent tester will remove the file from the test set… and then send it to a friend.

It is easy to understand why the user may think they have the rabbit virus and that the scanners that did not detect it are not as good as the scanners that detected it. And so a myth is born.

MYTH 1: VIRUSTOTAL CAN BE USED TO PERFORM COMPARATIVE TESTING

Rabbits are just one of the reasons why *VirusTotal* cannot be used for comparative testing. I will leave it to *VirusTotal* to explain some more of the reasoning for this.

> 'BAD IDEA: VirusTotal for antivirus/URL scanner testing
>
> 'At VirusTotal we are tired of repeating that the service was not designed as a tool to perform antivirus comparative analyses, but as a tool that checks suspicious samples with several antivirus solutions and helps antivirus labs by forwarding them the malware they fail to detect. Those who use VirusTotal to perform antivirus comparative analyses should know that they are making many implicit errors in their methodology, the most obvious being:
>
> 'VirusTotal's antivirus engines are commandline versions, so depending on the product, they will not behave exactly the same as the desktop versions: for instance, desktop solutions may use techniques based on behavioural analysis and count with personal firewalls that may decrease entry points and mitigate propagation, etc.
>
> 'In VirusTotal desktop-oriented solutions coexist with perimeter-oriented solutions; heuristics in this latter group may be more aggressive and paranoid, since the impact of false positives is less visible in the perimeter. It is simply not fair to compare both groups.
>
> 'Some of the solutions included in VirusTotal are parametrized (in coherence with the developer company's desire) with a different heuristic/agressiveness level than the official end-user default configuration.
>
> 'These are just three examples illustrating why using VirusTotal for antivirus testing is a bad idea.' [8]

Most of the rest of the myths I describe are components of the comparative testing myth, but each is applicable to the common use of *VirusTotal* for purposes other than misguided product testing. These points are important for the individual user to understand as well.

MYTH 2: DETECTION OF MALWARE ON VIRUSTOTAL MEANS THE SCANNER HAS DETECTION OF THE MALWARE

VirusTotal displays what a product says it detected. This does not mean that the scanner *would* detect that threat if it was on your computer. As *VirusTotal* explained, the vendors are free to configure their products as they wish to. It is not as simple as trying to configure your product the same way. A vendor can use undocumented switches to obtain heuristic detections that the user cannot. Although *VirusTotal* explains that heuristics may be different between perimeter solutions and desktop solutions, a command-line scanner can behave differently from either a desktop or perimeter solution. Vendors can configure cloud detections in a manner that only detects scans from *VirusTotal* (or a test lab).

In some cases a sample is detected by its wrapper alone. The actual threat inside the wrapper may not be detected. If the malware is present outside of its wrapper, then it may not be detected.

MYTH 3: LACK OF DETECTION ON VIRUSTOTAL MEANS THE FILE IS SAFE

Of course malware evading all virus scanners is extremely common. I do not need to explain that to this audience. (This audience needs to explain that to their non-technical friends and family.)

I am referring to a situation in which the presence of a clean file is indicative of the presence of harmful files. Although the file itself is harmless, the presence of the file is likely to indicate the user is in a dangerous situation. I will describe a file in this category later in this paper.

MYTH 4: LACK OF DETECTION ON VIRUSTOTAL MEANS THE SCANNER DOESN'T DETECT IT

In some cases a vendor withholds displaying detection of a threat. At times it may be advantageous to have detection in the product on your desktop, but not to display detection on virus-scanning services that malware authors may use to determine if their application is being detected. In other cases detection of the threat is irrelevant due to other technologies that prevent infection without naming a threat.

MYTH 5: FALSE POSITIVE MEANS FALSE POSITIVE

The same factors that make *VirusTotal* unsuitable for comparative testing may affect the proper interpretation of false positives too. Often, stronger heuristics mean there will be more false positives. In the workspace a false positive can cost an enterprise a lot more than a missed detection. On a consumer machine false positives increase vendor support costs and decreases user satisfaction with their product. *VirusTotal* can serve a vendor well as a testbed for new heuristics prior to public release of the new technology. A vendor once explained to me that they would sometimes test new heuristics on their free consumer products before adding them to their enterprise offerings. *VirusTotal* can help to replace human guinea pigs.

MYTH 6: MORE IS BETTER

Researchers and the media alike will frequently report that there is good, bad, or fair coverage of a threat submitted to *VirusTotal*. There is a difference between detection and protection. Detection of a threat by 45 out of 60 scanners does not mean that more people are protected from the threat than one which is detected by 10 out of 60 scanners. The reasons for this are market share (by number of users) and, less frequently, geography. If five out of 55 product detect a threat, and they are the five with the largest market share, then more users will be protected against the threat than if 30 scanners with minimal market share detect a threat and any of the top five scanners miss it.

According to the *OPSWAT* April 2017 market share report[3], the 10 *Windows* virus scanners with the most users account for 84.25% of the market share. The top four scanners were used by 50.83% of the user base. As long as the five scanners holding the majority of the market share detect a threat, then all of the rest of that set of scanners can miss the same threat and the majority of users will still be protected. The scanners with the largest market share may be significantly different in different geographical locations, for example China. If the top Chinese scanners miss a common threat in China, the top scanners in the rest of the world are likely to be relatively inconsequential. When a piece of malware is rarely seen outside of a specific country, as has previously been the case with some malware seen in Japan, the market share of the top scanners in that country may be the only meaningful measure of global protection metrics.

In the following examples would the detection ratios be considered good coverage? Bad coverage? Fair coverage?

Figure 3: HaoYu.exe was detected by 48 of 57 scanners.

In Figure 3, we see that HaoYu.exe was detected by 48 of 57 scanners, but look at who appears to have been missing detection at that time.

Figure 4: Symantec was missing detection of HaoYu.exe.

If *Symantec* had detected the file and 30 scanners that did detect the file had missed it, more people may have still been protected than what would appear to be the case in this example.

At this point it becomes essential to emphasize another difference between detection and protection. Security suites, such as that which *Symantec* offers, may not detect the file on *VirusTotal*, however their users may still be protected from the threat by other components of the product. This applies to many products, so even the number of protected users cannot be determined solely by the market share and number of products detecting a threat on *VirusTotal*.

Four out of 57 scanners display detection for the sample shown in Figure 5. Is that bad detection?

Based on three out of the four products referring to the file as adware, one would be inclined to say it is irrelevant, however a year later this sample was detected by 18 products. The composition of the detection types still favours adware or riskware, but a test lab could potentially defend the inclusion of

[3] *OPSWAT*'s demographics cannot be extrapolated to the enterprise market share. Due to the sample set *OPSWAT* uses there will be significant differences in worldwide metrics.

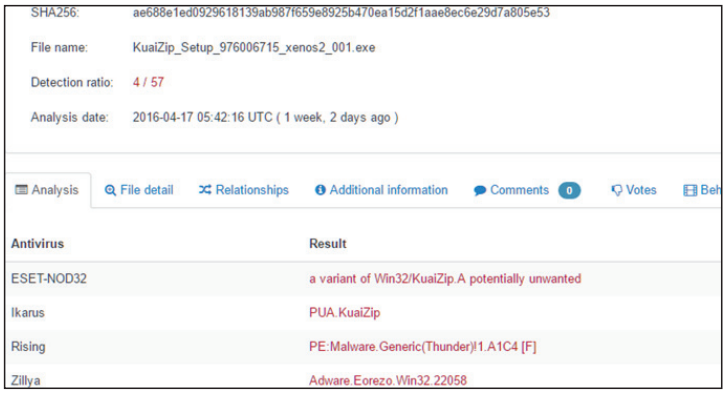

Figure 5: Four out of 57 scanners display detection.

this file in a comparative test set. The file communicates with IP addresses known to have hosted actual malware. In a testing situation where dynamic execution resulted in the download and execution of malware, the sample can reasonably called malware. Obtaining the application from the developer's website can be tricky since some AV products and browsers block the site itself. While there are times that a designation of adware, etc. is based upon legalities, vendor reputation, or even a risk analysis of the prevalent use of the file for benevolent purposes, in some cases the risk to consumers is such that a failure to provide any detection is undeniably harmful. Based upon the market share of the scanners detecting this specific file, coverage on *VirusTotal* is poor at best.

How is the coverage on the following file?

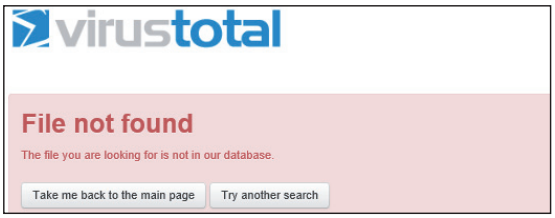

Figure 6: File not found.

Looking at *VirusTotal* alone that day there was no way to determine if the file was clean, or even if the file was detected by all of the scanners. In the case of this specific file, coverage on *VirusTotal* was almost certainly abysmal. *NSS Labs Baitnet* discovered this file on 6 June 2017. *OPSWAT*'s *Metadefender* had seen the file on 4 June and only three of 39 scanners detected the threat at the time of this scan on 5 June (Figure 7). On 9 June *VirusTotal* indicates that 34 out of 61 products detected the file.

Based on the relationship to an exploit, *OPSWAT*'s detection information and timing, as well as information indicative of when most scanners on *VirusTotal* reported detection, it is reasonable to believe that prior to 9 June very few anti-virus scanners were able to detect the threat.

MYTH 7: MALICIOUS WEBSITE MEANS MALICIOUS WEBSITE

Legitimate websites are frequently compromised and may contain exploits, host phishing pages, or host malware. Maryhill Manor (Figure 8) is one such example.

The scan results of http://www.maryhillmanor.org (Figure 9) show the site is detected as malicious or suspicious by some

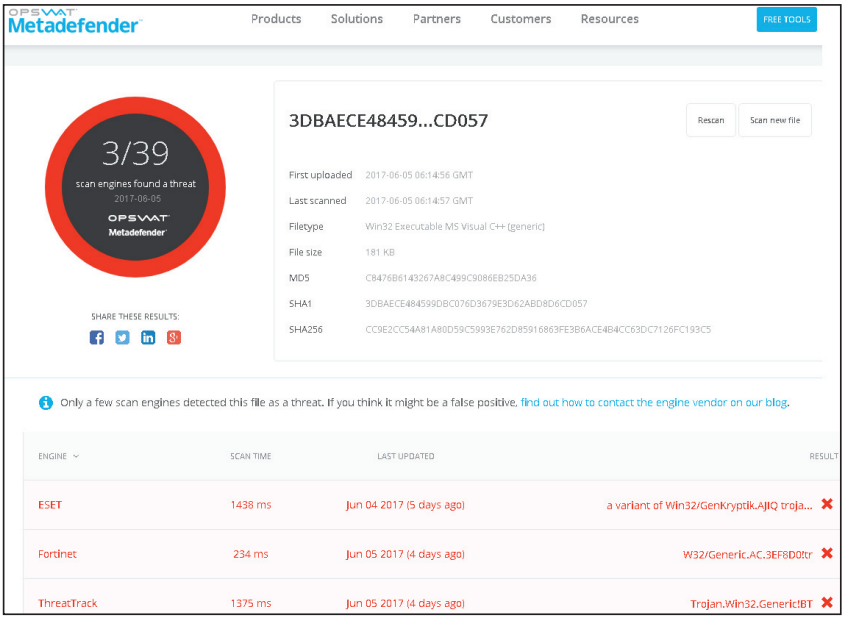

Figure 7: Only three of 39 scanners detected the threat at the time of this scan on 5 June.

Figure 8: Maryhill Manor.

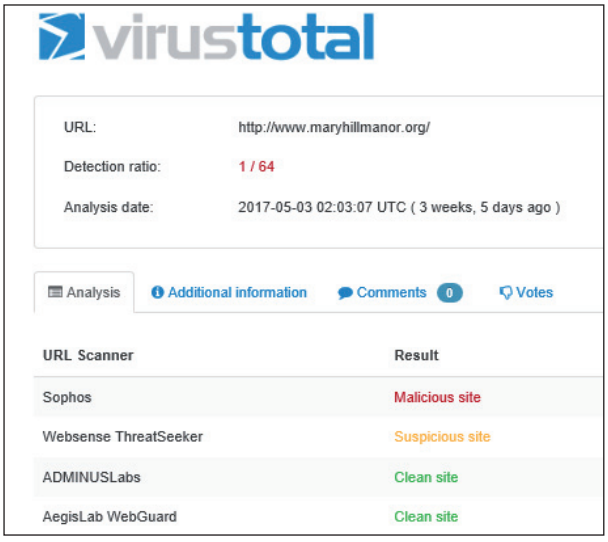

Figure 9: The Maryhill Manor site is detected as malicious or suspicious by some products.

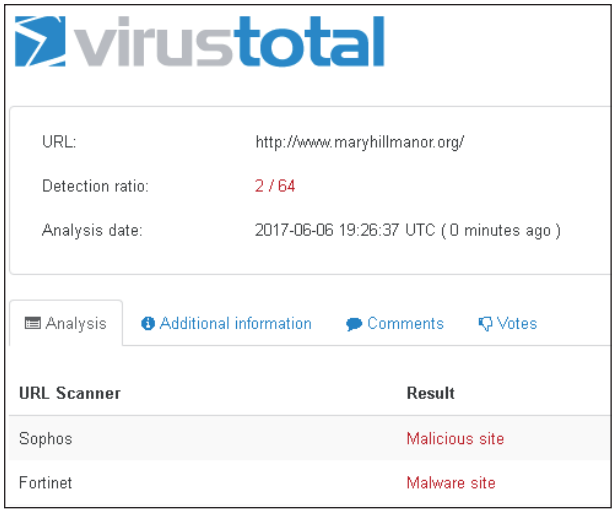

Figure 10: A scan of the Maryhill Manor site a month or so later.

products. At various times I have seen anywhere from one to six products reporting the site as unsafe. Maryhill Manor is a legitimate health care facility with a legitimate website. The problem is that the site has been compromised on several occasions.

The scan shown in Figure 10 was a month or so after the previous scan (Figure 9) and the results are a little worse.

Once a site has been identified as hosting exploits, malware or phishing attacks, it can take a long time for scanners to remove detection. As is the case with most scans, *VirusTotal* does provide more contextual information about URL scans.

BEYOND THE SCAN REPORTS

Once the results of a scan are returned there are tabs containing information that can enhance one's understanding of the nature of the threats. Not all tabs will be provided for every submission. Brand new submissions would be expected to have less contextual data available.

Typically, there is less forensic information returned from URL scans than file scans, however on the 'Additional Information' tab the IP address resolution and scanning engine details can be found.

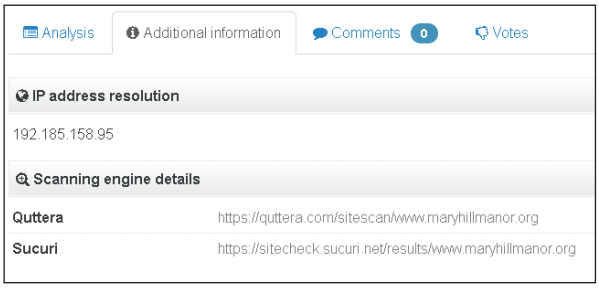

Figure 11: The IP address resolution and scanning engine details can be found under the 'Additional Information' tab.

The scanners listed under 'Scanning engine details' provide hyperlinks that will initiate a new scan and return information such as geolocation information or whether the site is blacklisted, etc.

Typically, there will be far more information available from a file scan than from a URL scan. This information can be of assistance in understanding the technical details of the sample and in adding context to it.

Earlier in this paper I mentioned that even if a file is safe, its presence may indicate an unsafe situation. In the following example I will use information provided by *VirusTotal* to address the myths that state 'Lack of detection means the file is safe' and 'False positive means false positive'. I have provided the URL for the example being discussed for readers who may wish to try some of the techniques used:

https://www.virustotal.com/en/file/43239bce0a3200c5d61d968f8e130dbaa3bf987e02417d49191c72bbf1636d4e/analysis/

This specific version of ravmond.exe, is a component of an older version of a legitimate Chinese anti-virus product.

Bkav is a large security company in Vietnam. *Bkav* was the only scanner to report the file as adware or anything at all (Figure 12). Is this a case of a false positive? Let's dig a bit deeper. We will start with the 'File Detail' tab, shown in Figure 13.

Figure 12: Bkav was the only scanner to report ravmond.exe as adware or anything at all.

Figure 13: File details.

Further down on the 'File Detail' page (not pictured) there is information about attributes of the PE file, as well as debug information.

The file is digitally signed and timestamped, although it appears to be for a 2012 anti-virus product. Other research I have done supports the conclusion that the certificate is in order. This is one contextual component of our analysis that tends to support a conclusion of a false positive detection. There is not enough evidence to draw a conclusion at this time.

Carbon Black provides some interesting information on the 'Relationships' tab. Details include the hashes of files that wrote this sample to disk, hashes of the files that the sample wrote to disk, files that were running at the time the samples were written to disk, the overlay parents. Hashes provided are hyperlinked, however some of the related files have not been submitted to *VirusTotal*. *VirusTotal* also reports on compressed bundles that the sample was included in.

Carbon Black reported it had seen eight files that wrote this sample to disk. A couple of the files were not present on *VirusTotal* and one to 13 scanners displayed detections for each of the other samples.

This sample of ravmond.exe wrote 50 files to disk. These files appear to be clean and part of the *Rising Antivirus* product. There is still nothing that indicates that this sample is malicious.

There is something interesting when you get down to the execution parents, as shown in Figure 14.

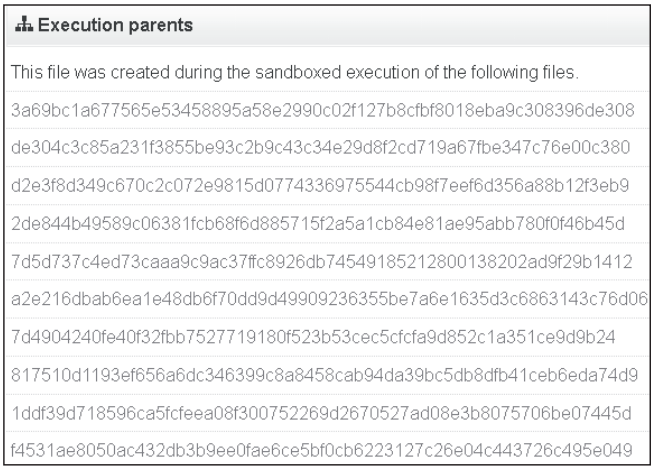

Figure 14: Execution parents.

The hashes shown in Figure 14 are from just a few of the execution parents. There were 50 files in all that *Carbon Black* reported as execution parents. Many, if not all of these files were detected by multiple scanners as adware, PUPs, or malware. One of the execution parents was particularly interesting in that it was detected by *AVG* as 'Beijing Rising Information Technology Corporation Limited'. The file was digitally signed, however the digital signature did not verify (MD5: 4ee6cfd6ca6c2e172095f2ca016d9e02). It is rare to identify malware by the name of a large security vendor, but I have encountered this detection name on a different sample with a verified signature. Another execution parent was

detected by *VBA32* as Signed-Adware.Hao123.BaiduBeijingCo (MD5: fc234b76a106b8fd1f1abc30e43270d0f72da1ab).

There is a tab containing additional information about files, such as file identification hashes, file size and type, etc. There is a list of different filenames the ravmond.exe sample being discussed has been has been seen with, but those may have been renamed by researchers prior to being uploaded. For example, 'vt-upload-Zdl8aB' is not likely to be a name that the file was seen as in the wild. Under behaviour characterization, *Zemana* reports dll-injection.

This file was dropped by an exploit and was one of several files dropped at the same time. The file was obviously part of a bundled software package that contained malware. *Bkav* was the only one out of 61 scanners to detect the sample. From the information provided by *VirusTotal* via *Carbon Black*, this file is frequently bundled with malware. The presence of the file on a computer that is not running a Chinese version of *Windows* is quite likely to indicate the presence of malware on the system. *Rising Antivirus* will not install on anything but a Chinese version of *Windows*. If a virus scanner detects the presence of this file on a computer that is not using the Chinese version of *Windows*, it is reasonable to detect the file. If the file is found on a computer in China, and was not installed from the *Beijing Rising* website, it may be surrounded my malware as well. If the file is legitimately present, *Beijing Rising* is unlikely to detect it as malware, but may suggest the user install a newer version of the product. It is entirely possible for *Bkav* to omit detection from computers running a Chinese version of *Windows*. The safe file itself is an indication of danger on most computers. Just because this file is not detected it doesn't mean it is any safer than a good piece of cheese in a mousetrap is for a rodent. Detection of the file may be an unintentional false positive by *Bkav*, but this detection can be quite useful.

VOTING AND COMMENTARY

VirusTotal allows for voting on the safety of a file, as well as commenting on a file. As a rule, the voting is of no value. Empty zip files, operating system files, and many other obviously clean files will often have votes indicating the files are malicious.

Comments will sometimes provide other third-party analysis and may be of value in those situations, however comments like 'it's a bad file' are often related to false positives, and of course add no value.

A FEW CLOSING REMARKS

File and URL scanning are components of multiple security products. The *NSS Labs Cyber Advanced Warning System* (*CAWS*), *ReversingLabs TitaniumCore* and *OPSWAT Metadefender* are just three examples of products that provide threat-scanning services, but only as a portion of more comprehensive security offerings. *VirusTotal* does not perform threat modelling or continuous incidence response, or data sanitization. If you believe a company offering threat submission and scanning services is like *VirusTotal*, look again at the complete offerings of that company before you attempt to make a determination. As *VirusTotal* has explained, it does not replace other security solutions.

VirusTotal is loved by users of all skill levels and throughout the world. Despite frequently incorrect conclusions, users do protect themselves from the installation of adware which may lead to more serious system compromise – and often, unsupported conclusions are correct anyway.

VirusTotal is also an important part of the security ecosystem. The bilateral information sharing with the security industry helps make the Internet safer for all of us.

REFERENCES

[1] https://www.virustotal.com/en/documentation/email-submissions/.

[2] https://www.virustotal.com/en/documentation/browser-extensions/.

[3] https://www.virustotal.com/en/documentation/desktop-applications/.

[4] https://www.virustotal.com/en/documentation/mobile-applications/.

[5] https://www.virustotal.com/en/documentation/public-api/.

[6] https://www.virustotal.com/en/faq/#virustotal-api.

[7] https://www.virustotal.com/en/documentation/private-api/.

[8] https://www.virustotal.com/en/about/.