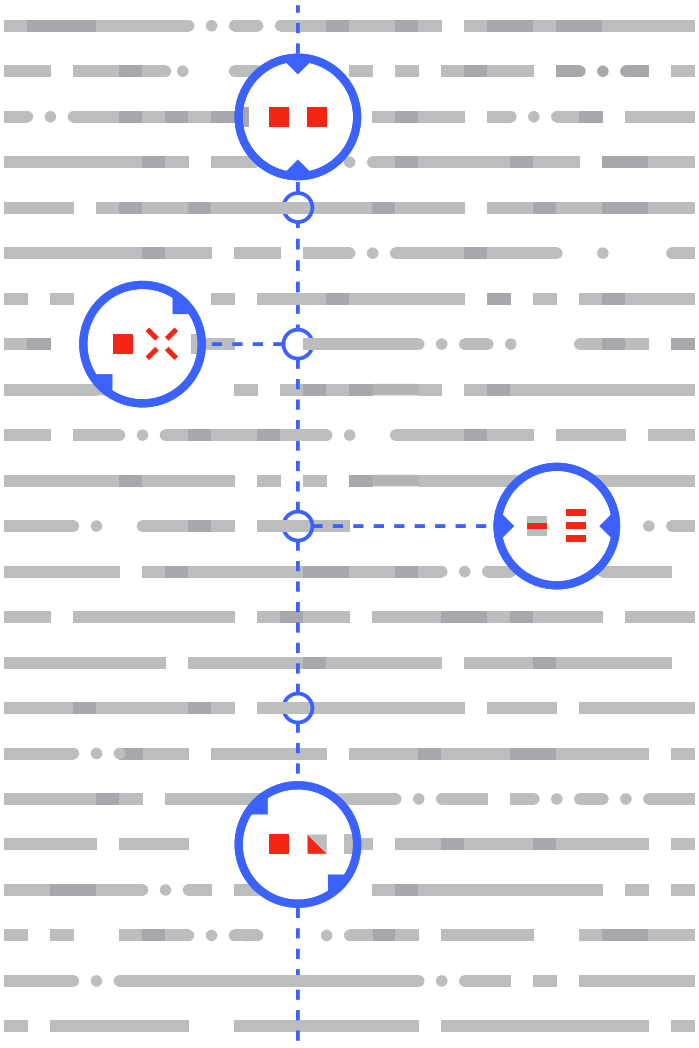
VTI for Threat Investigations

How to use VirusTotal Intelligence to investigate malware threats within your network

VirusTotal Intelligence provides extensive information to accelerate malware threat investigations. Analysts can quickly build a picture of an attack and then use the information to better protect against other attacks.



In the course of an investigation, security analysts and incident responders are often presented with a file hash and asked to make sense of an attack. Unfortunately, this is like being given only a bullet and then asked to uncover an entire plot. Without further context, it is virtually impossible to perform attribution, build effective defenses against other strains of the attack, or understand the impact of a given threat on an organization.

For example, your corporate AV solution or network defenses might have blocked the file

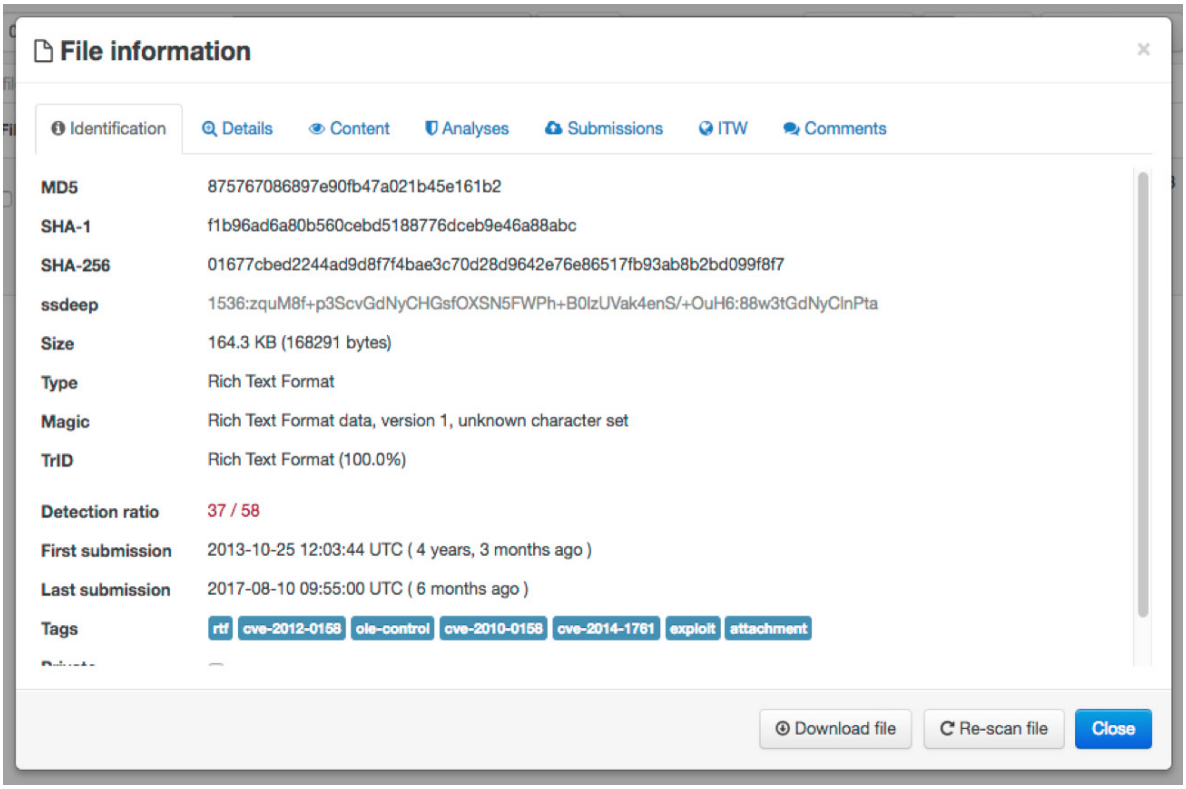
01677cbed2244ad9d8f7f4bae3c70d28d9642e76e86517fb93ab8b2bd099f8f7

from entering your network. However, it is impossible to know much about the attackers behind this incident and their intentions from this alone.

VirusTotal Intelligence (VTI) allows a threat analyst to access the entire VirusTotal collection of nearly 2 billion files spanning back to 2006, making them easily searchable via more than 40 search modifiers, acting as both a telescope into malicious behaviors on the Internet and a microscope to dissect individual pieces of malware.

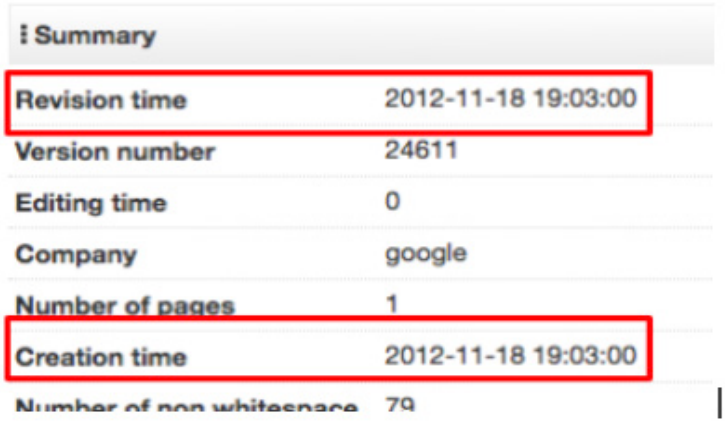
To better understand the scope of information within VTI, let's enter the hash above in VirusTotal Intelligence and examine the details VTI returns:

https://www.virustotal.com/intelligence/search/?query=01677cbed2244ad9d8f7f4bae3c70d28d9642e76e86517fb93ab8b2bd099f8f7



The malware sample's profile enables us to identify the file quickly (file type and size, hashes, key submission dates, etc.). In this case, it's clear that this is a Rich Text Format (RTF) document, and by looking at the sample tags we see that the document is probably exploiting the vulnerability described by CVE-2012-0158, to abuse the victim's machine and deploy further malicious code.

VirusTotal Intelligence runs files through multiple antivirus solutions on files, but it also processes every file upload (over 1 million per day) with a myriad of tools, to extract further metadata and interesting suspicious signals: ExifTool, PDFiD, oletools, pefile, etc. The resulting information allows an analyst to dig more deeply into techniques used by attackers. In this particular case, rtfinspect, a tool developed in-house by VirusTotal, allows us to estimate the creation date of this threat.

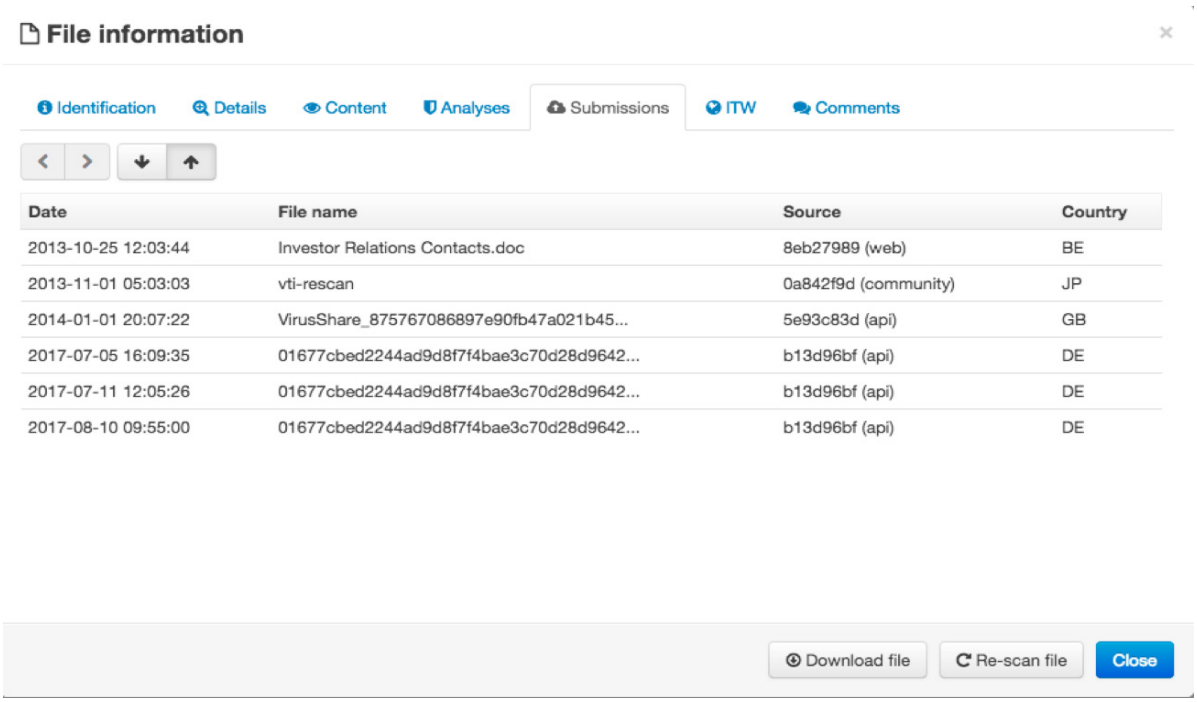


The file details tab in Intelligence displays the output of different tools when acting on a file

Similarly, the VTI advanced toolset can often indicate who a given attacker is trying to impersonate, using, for example, the authenticode signature information of a Windows executable. In this particular case the document metadata reveals that the attacker has set "Google" as the file creator's company. We can then use these artifacts to pivot to other attacks by the same group:

metadata:"google" type:rtf metadata:"OLE control"

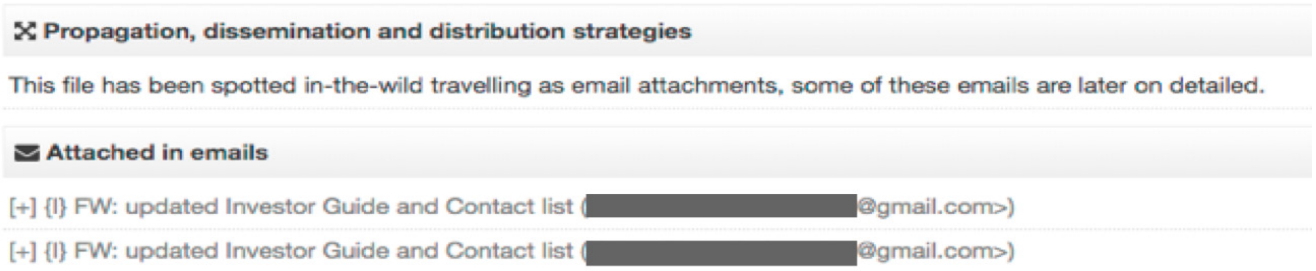
As we traverse the different file profile tabs, it's possible to explore how detection of this malware has evolved. We can also see all uploads of the threat to VirusTotal:



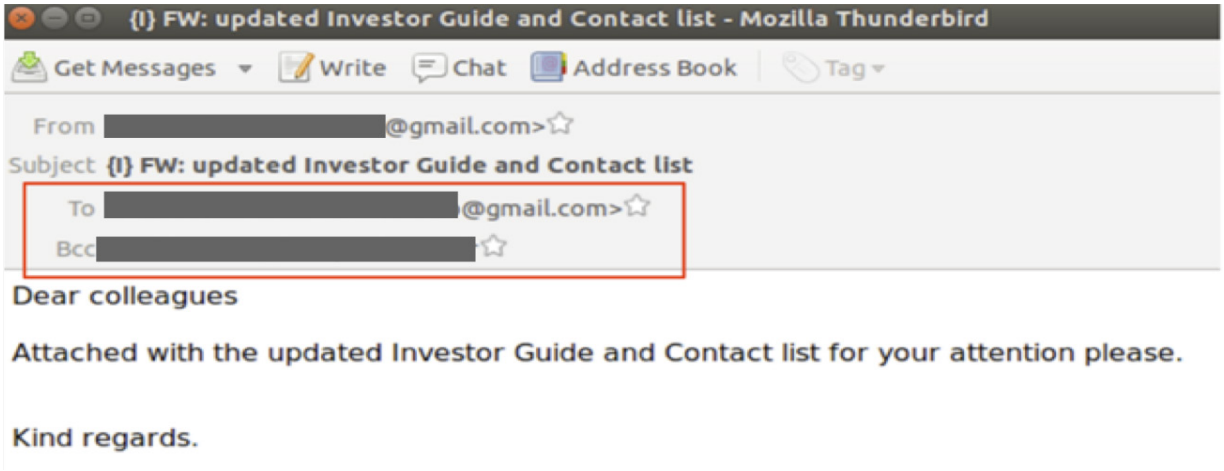
We can now confirm the timeline for the attack and can begin to understand the techniques used to deceive this sample's victims. The file was uploaded to VirusTotal with the name "Investor Relations Contacts.doc;" perhaps the victim was spear phished and tricked into opening the infected file, thinking it was some type of financial document. Furthermore, it appears that the first upload of this file came from Belgium -- perhaps the victim was located there. The submission metadata can be used to build a picture of regions where a given threat is prevalent.

The in-the-wild (ITW) tab provides the final pieces of this puzzle. This tab contains all the relationship information that VirusTotal Intelligence builds behind the scenes for files. Whenever users upload compressed bundles to the service, the bundles will be uncompressed and inspected, building parent-child relationships in the process. The backend VTI processes also scan every submitted URL to download its content and add in-the-wild download points for files that are already present in the database. As VTI executes files in detonation sandboxes, it also builds parent-child relationships for new files that might be dropped into a network. Tools such as Microsoft Sysinternals contribute end-user machine creation dates and paths for threats. A long list of backend VTI processes ensures that files do not appear as isolated "bullets" in our dataset, but instead are connected to other bullets, victims, guns, bad actors, etc.

In this particular case, the in-the-wild tab reveals that the file under study was seen as an attachment in an email that had previously been uploaded to VirusTotal:



We can now pivot to the email that contained the file, to understand which language and tricks the attacker used to deceive its victim:



Here we can see not only that the attack posed as a financial document, but also that it tried to compromise an executive of large European bank.

Now that we have filled in the gaps for this particular threat, it is time to understand more about the actors behind it. Are they targeting other victims and sectors? Is this an ongoing effort? Have we observed any network infrastructure that distributes these threats? What are the deception techniques used in other campaigns?

VirusTotal Intelligence allows you to search for similar files via several mechanisms:

- A feature hash that clusters together files exhibiting similar structural and binary patterns
- imphash
- Ssdeep
- Modifier based searching for distinctive metadata attributes

If we launch a file similarity search we immediately get to dozens of related files worth studying:

Similar-to:01677cbed2244ad9d8f7f4bae3c70d28d9642e76e86517fb93ab8b2bd099f8f7

It is an easy next step to create a script that uses VirusTotal's Private API to process this data and extract patterns and commonalities. These allow us to add more detail to the adversary profile under construction. The script can launch the same file-similarity search above, making use of the search API. For each match, it can retrieve all sample details programmatically with the file lookup API. In this way, we can automatically discover that the attackers are using other spam campaigns with similar malicious payloads and different subject lines and bodies:

- NSA Secrets: Snowden latest revealed (Snowden.doc)
  - fb76b445a5dda5e22cdfc80be7e35c8b99f8ff705f5e8cc767b4b1c8b1cd72ac
- Glenn Greenwald, Associate of Edward Snowden, talked to "MK" about his revelatory book (SnowdenBook.doc)
  - 88f9a4ad25ab90fe844256d159232c600dd1537ba13462dcd58c1783ffaf85c2

The analysis also shows that the attackers are targeting Government officials from Israel. Other submission file names also confirm that the main vehicle used by this actor in order to target its victims are spear phishing campaigns:

Updated contact details for Mission.doc
Snowden.doc
ISB working note H.E..doc
Draft letter.doc
SnowdenBook.doc
Conferences.doc

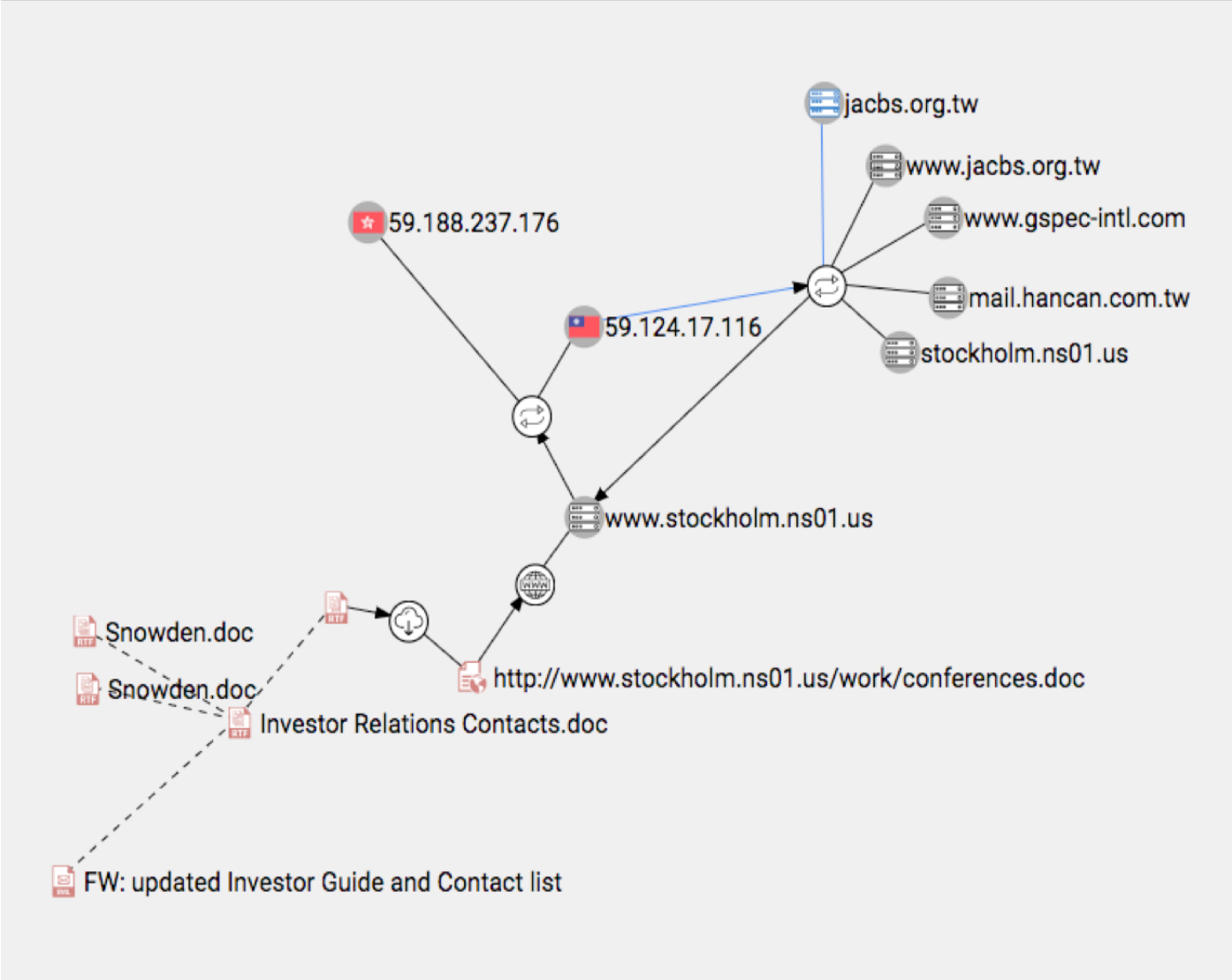
We also discover that other variants of the same threat were once seen being downloaded from:

http://www.stockholm.ns01.us/work/conferences.doc
D44f6219cee5ce5397f3edffaaf0c1bce29320fb00507732e25859c84aec1c7f

Thanks to VTI's network location-related reports, we may continue pivoting and digging even further, to continue adding detail to the picture:

https://www.virustotal.com/#/domain/www.stockholm.ns01.us

We can record our findings in a VirusTotal Graph that we can share with colleagues and other researchers, to present our discoveries and collaborate on the on-going investigation:



Now with a collection of similar files likely pertaining to the same actor, we can write a Yara rule in VTI Malware Hunting, to keep tabs on the group, be notified about new campaigns by the same group, and understand the evolution of their tactics, techniques and procedures. Moreover, these rules can then be deployed in our organization's prefered security solutions, to add additional layers of protection.