Never upload ransomware samples to the Internet

0xc0decafe.com/2020/12/28/never-upload-ransomware-samples-to-the-internet/

December 28, 2020

Ransomware is our contemporary plague. It is a thriving business that attracts more and more cybercriminals every month. New ransomware gangs sprout like mushrooms. These self-proclaimed “security teams” test the security of many small to large enterprises. But their unsolicited penetration tests are not that cheap. What they leave behind is pure mayhem and a huge bill for the victims. Furthermore, some attacks are really disgusting since ransomware gangs have targeted non-profit organizations, schools, and even hospitals on various occasions.

There are hundreds of articles on the Internet about ransomware. For instance, the No More Ransom project educates on ransomware and offers help for victims. There are technical approaches to stop ransomware. Of course, the cyber security industry offers many products to protect against or mitigate ransomware. There are also community approaches like Raccine that help to stop ransomware.

But once ransomware has been deployed on your network and you are in a ransomware incident, the headless chicken mode is very common. Unfortunately, there is one golden rule that I often see getting broken due to headless chicken mode:

> NEVER EVER upload ransomware samples to the Internet!
>
> *Some random incident responder*

Even though I thought that this would be common knowledge, I’ve been proven wrong many times. Therefore, this is my take at explaining what information a ransomware sample contains, why you should never upload them to the Internet, and what actually happens if you upload them after all.

Audience: This is definitively not an article for the seasoned Cyber Threat Intelligence analyst or the alike. This is an article dedicated to the ones in many smaller to medium businesses, schools, hospitals, and so on that do not have a dedicated security team: the non-security IT staff including system administrators that are typically the firsts to encounter the mess ransomware gangs leave behind. But also entry-level cyber security professionals can benefit from reading this article and understand how analysts hunt for ransomware samples.

What kind of information does a ransomware sample contain?

Ransomware is only the last step of a network intrusion. It may have started with a spear-phishing mail, later on, some undetected lateral movement, and subsequently the take over of your Windows Domain Controller. At this point in time, the attacker may deploy the ransomware on the network on a lonely Friday night.

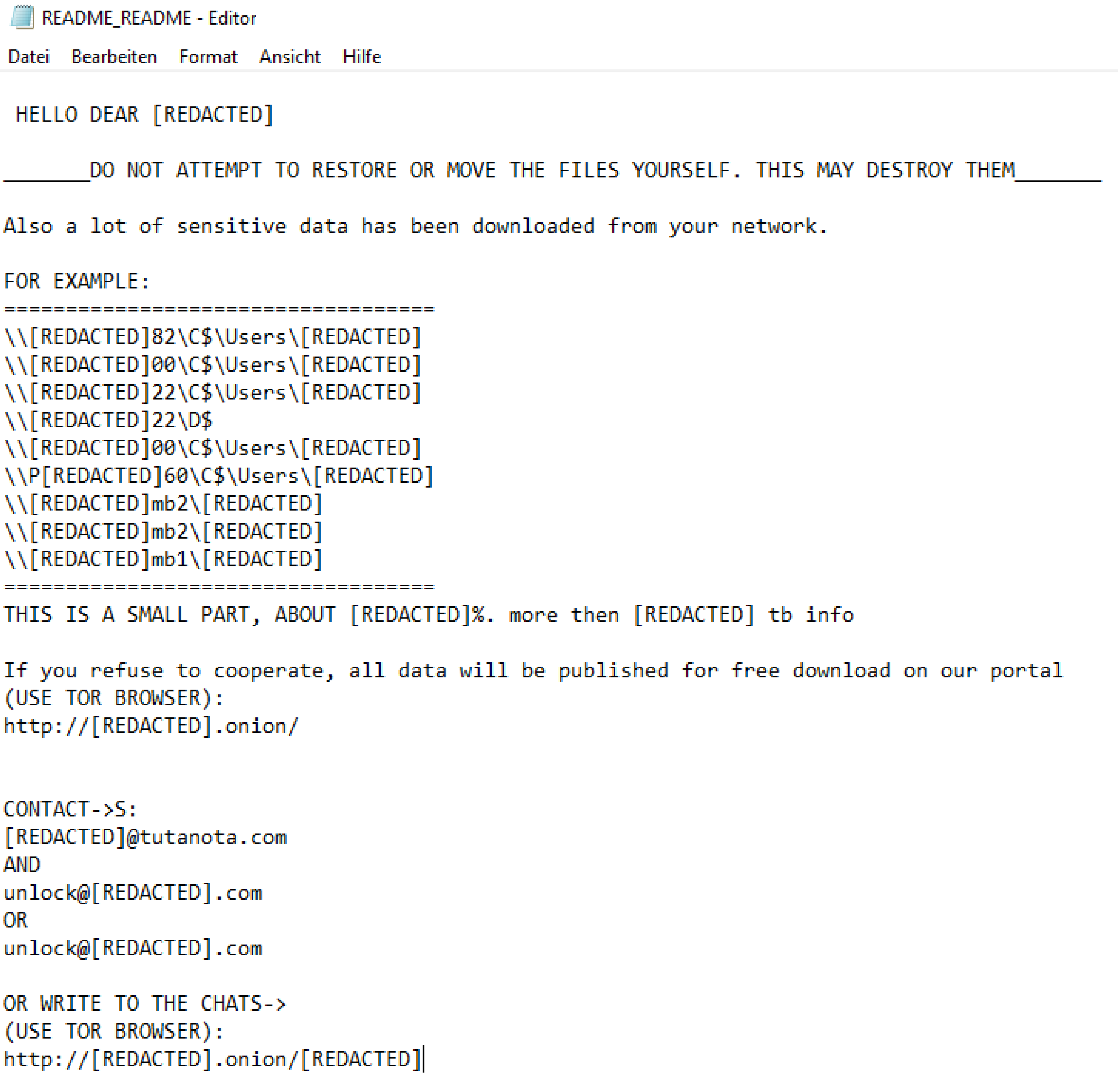
These ransomware samples are often compiled for the victim at hand. They are therefore *unique*. Hence, they contain a lot of information related to the victim that should not be made public. This information includes:

- a ransom note with

    the name of the victim
    - names of network shares
    - names of computers in the network
    - names of employees (as part of network share paths)
    - names of clients
    - type of stolen data (e.g. accounting data, executive data, …)
    - links to screenshots as proof (e.g. data listings, bank account balances, …)
- meta-information

    the timestamp of the ransomware sample that can be used to estimate the date of the attack

The following ransom note that I’ve extracted from a ransomware sample uploaded to the Internet illustrates my point:



```
 HELLO DEAR [REDACTED]

_______DO NOT ATTEMPT TO RESTORE OR MOVE THE FILES YOURSELF. THIS MAY DESTROY THEM_______

Also a lot of sensitive data has been downloaded from your network.

FOR EXAMPLE:
===================================
\\[REDACTED]82\C$\Users\[REDACTED]
\\[REDACTED]00\C$\Users\[REDACTED]
\\[REDACTED]22\C$\Users\[REDACTED]
\\[REDACTED]22\D$
\\[REDACTED]00\C$\Users\[REDACTED]
\\P[REDACTED]60\C$\Users\[REDACTED]
\\[REDACTED]mb2\[REDACTED]
\\[REDACTED]mb2\[REDACTED]
\\[REDACTED]mb1\[REDACTED]
===================================
THIS IS A SMALL PART, ABOUT [REDACTED]%. more then [REDACTED] tb info

If you refuse to cooperate, all data will be published for free download on our portal
(USE TOR BROWSER):
http://[REDACTED].onion/


CONTACT->S:
[REDACTED]@tutanota.com
AND
unlock@[REDACTED].com
OR
unlock@[REDACTED].com

OR WRITE TO THE CHATS->
(USE TOR BROWSER):
http://[REDACTED].onion/[REDACTED]
```

Example ransom note containing a lot of information about the victim

Needless to say that this information should not turn up on the Internet. I know that some will argue that this information will be public soon anyway if the victim does not pay the ransom. Because modern ransomware gangs use the double extortion tactic. In a nutshell, before deploying the ransomware, these gangs steal (sometimes) terabytes of data from a network and threaten to publish this information on the Darknet or sell/auction it off.

By the way, paying the ransom is something that is never recommended. Above all, because this proves to cybercriminals that this is an effective way of making money. Furthermore, this may have severe consequences for a business, if it pays cybercriminals residing somewhere in an embargoed region.

Why shouldn’t I upload ransomware samples to the Internet?

As you’ve seen, there is a lot of information related to the victim that a ransomware sample contains. Once IT staff is confronted with a ransomware incident, they may start their own investigation, trying to find the root of all evil. One of these steps is typically uploading many of the suspicious files found on the network to online services like VirusTotal. Consequently, these samples are public on the Internet.

Unfortunately, this is a common mistake that IT staff unaware of cyber security subtleties commits. What do you gain by uploading ransomware samples? You probably know already that the sample at hand is malware because it encrypted most of your network. Often the classification of the malware, if that really matters at this particular moment, is often proudly presented by the malware itself. Either as a file extension of all the encrypted files or in the ransom note. Therefore, you are not gaining anything, but possibly losing a lot.

Services like VirusTotal are very good to check if a file is malicious and you suspect that it is commodity malware. Therefore, the first step is never to upload a file but rather check its file hash, e.g. sha256. Somebody else usually has uploaded the sample for us anyway. There are great tools like malwoverview that help you with this task.

If a hash does not yield a result then there are several explications. First, the sample is too fresh that somebody has uploaded it yet, check back a couple of minutes later. Second, the threat actor uses hash busting and changes the hash of each sample. Third, this sample is unique because it was utilized in a targeted attack.

The third point is the point that applies to ransomware. The sample is *unique*. Ransomware threat actors compile their samples typically for each victim just before the deployment. Even though this is not a nation-state actor that attacked your network, you should treat the sample as if it were from one due to the information leakage that would occur on upload.

Even though not uploading ransomware samples to the Internet won’t fix the core problem you may have, i.e. an encrypted network, this will likely make your (at this point in time miserable) life a little bit brighter.

Because you have much more time to focus on the actual incident and you do not have to deal with a media disaster right from the beginning! Perhaps this gives your press relations officer some time to prepare a proper statement.

Furthermore, note that this is a way to identify ransomware victims that paid the ransom and never showed up on any ransomware portal. The proof that they fall victim and paid will be out there forever. Mind the possible consequences I’ve stated above.

What happens if I upload a ransomware sample to the Internet?

There are many analysts out there that hunt for these samples for several reasons. One of them is not that noble but very common: public discussion of who got ransomwared by whom. This is then picked up by the press and it is something that you do not need when already in a ransomware incident, possibly in headless chicken mode anyway.

Let me illustrate by the example of VirusTotal what happens. The following applies to similar services on the Internet. I choose VirusTotal because it probably the most common choice of IT staff to upload malicious samples. It is not that I am blaming anything on this very useful service. Actually, VirusTotal tells you this in their Terms of Service, their Privacy Policy, and again right about the time you click on “Submit”:

> By submitting data below, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission.
>
> *VirusTotal*

So, you’ve been warned a lot!

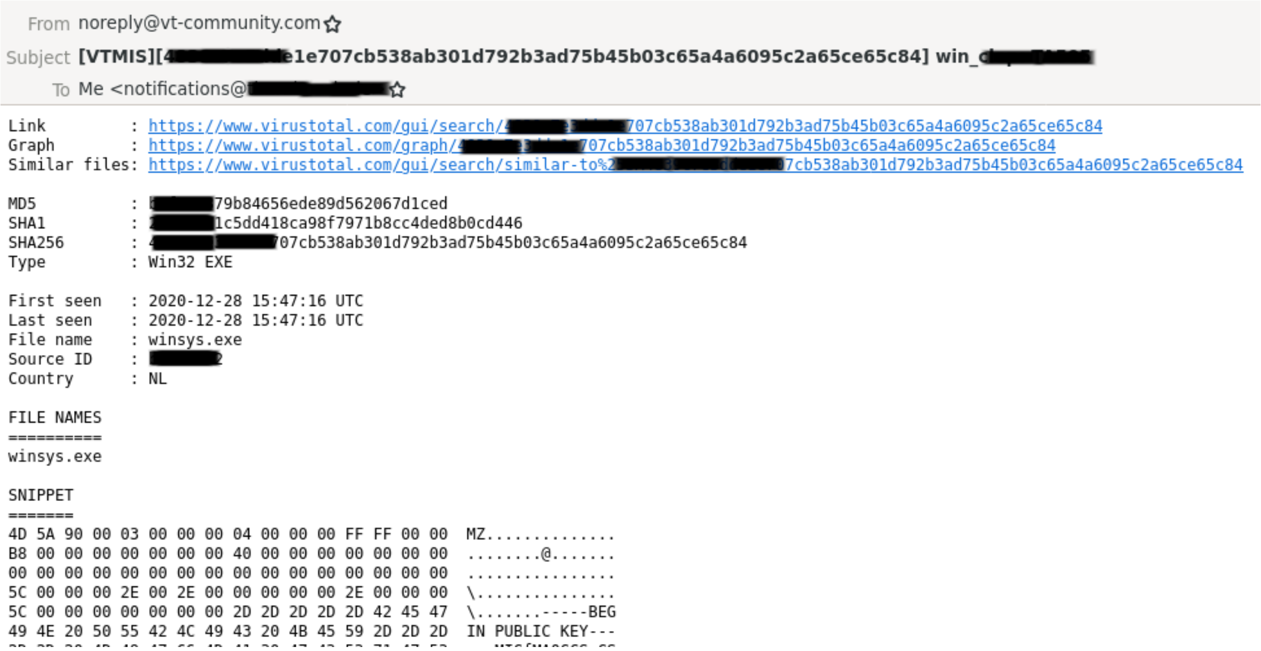
But you may ask: how do analysts find my sample in the endless stream of files uploaded to VirusTotal? This is where LiveHunt comes into play. This is a service that is offered to customers and researchers to hook into the never-ending stream of files uploaded. Each file is checked against custom signatures (YARA rules). Furthermore, these samples are shared with AV companies who will likely have other ways to find the needle in the haystack.

If you know exactly what you are looking then it is quite easy to find the needle in the haystack. This means once you have analyzed one sample of a certain ransomware family, written a YARA rule for it, then you will likely detect it in the future again. Actually, you do not have to write many rules on your own because there are plenty on Github. For instance, the following is a YARA rule for the ransomware family Ryuk:

```
rule Ransom_Ryuk_sept2020 {
   meta:
      description = "Detecting latest Ryuk samples"
      author = "McAfe ATR"
      date = "2020-10-13"
      malware_type = "ransomware"
      malware_family = "Ransom:W32/Ryuk"
      actor_type = "Cybercrime"
      actor_group = "Unknown"
      hash1 = "cfdc2cb47ef3d2396307c487fc3c9fe55b3802b2e570bee9aea4ab1e4ed2ec28"

   strings:
      $x1 = "\" /TR \"C:\\Windows\\System32\\cmd.exe /c for /l %x in (1,1,50) do
start wordpad.exe /p " fullword ascii
      $x2 = "cmd.exe /c \"bcdedit /set {default} recoveryenabled No & bcdedit /set
{default}\"" fullword ascii
      $x3 = "cmd.exe /c \"bootstatuspolicy ignoreallfailures\"" fullword ascii
      $x4 = "cmd.exe /c \"vssadmin.exe Delete Shadows /all /quiet\"" fullword ascii
      $x5 = "C:\\Windows\\System32\\cmd.exe" fullword ascii
      $x6 = "cmd.exe /c \"WMIC.exe shadowcopy delete\"" fullword ascii
      $x7 = "/C REG ADD
\"HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\" /v \"EV\" /t
REG_SZ /d \"" fullword wide
      $x8 = "W/C REG DELETE
\"HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\" /v \"EV\"
/f" fullword wide
      $x9 = "\\System32\\cmd.exe" fullword wide
      $s10 = "Ncsrss.exe" fullword wide
      $s11 = "lsaas.exe" fullword wide
      $s12 = "lan.exe" fullword wide
      $s13 = "$WGetCurrentProcess" fullword ascii
      $s14 = "\\Documents and Settings\\Default User\\sys" fullword wide
      $s15 = "Ws2_32.dll" fullword ascii
      $s16 = " explorer.exe" fullword wide
      $s17 = "e\\Documents and Settings\\Default User\\" fullword wide
      $s18 = "\\users\\Public\\" fullword ascii
      $s19 = "\\users\\Public\\sys" fullword wide
      $s20 = "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\"
fullword ascii

      $seq0 = { 2b c7 50 e8 30 d3 ff ff ff b6 8c }
      $seq1 = { d1 e0 8b 4d fc 8b 14 01 89 95 34 ff ff ff c7 45 }
      $seq2 = { d1 e0 8b 4d fc 8b 14 01 89 95 34 ff ff ff c7 45 }

   condition:
      ( uint16(0) == 0x5a4d and
      filesize < 400KB and
      ( 1 of ($x*) and 5 of them ) and
      all of ($seq*)) or ( all of them )
}
```

This rule comprises several strings and a condition that is checked against each file. The condition matches, roughly speaking, Windows binaries that are less than 400 kilobytes in size and comprise a certain number of the aforementioned strings.

Let’s say you uploaded a ransomware sample to VirusTotal, which belongs to one of the heavily tracked ransomware families then there are likely several YARA rules going off, and researchers notified. Notifications are either seen in the VirusTotal WebGUI or via email notification as shown in the following screenshot.



From noreply@vt-community.com ☆
Subject **[VTMIS][[redacted]e1e707cb538ab301d792b3ad75b45b03c65a4a6095c2a65ce65c84] win_[redacted]**
To Me <notifications@[redacted] ☆

```
Link         : https://www.virustotal.com/gui/search/[redacted]707cb538ab301d792b3ad75b45b03c65a4a6095c2a65ce65c84
Graph        : https://www.virustotal.com/graph/[redacted]707cb538ab301d792b3ad75b45b03c65a4a6095c2a65ce65c84
Similar files: https://www.virustotal.com/gui/search/similar-to%2[redacted]7cb538ab301d792b3ad75b45b03c65a4a6095c2a65ce65c84

MD5          : [redacted]79b84656ede89d562067d1ced
SHA1         : [redacted]1c5dd418ca98f7971b8cc4ded8b0cd446
SHA256       : [redacted]707cb538ab301d792b3ad75b45b03c65a4a6095c2a65ce65c84
Type         : Win32 EXE

First seen   : 2020-12-28 15:47:16 UTC
Last seen    : 2020-12-28 15:47:16 UTC
File name    : winsys.exe
Source ID    : [redacted]
Country      : NL

FILE NAMES
==========
winsys.exe

SNIPPET
=======
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..............
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ........@.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
5C 00 00 00 2E 00 2E 00 00 00 00 00 2E 00 00 00  \...............
5C 00 00 00 00 00 00 00 2D 2D 2D 2D 2D 42 45 47  \.......-----BEG
49 4E 20 50 55 42 4C 49 43 20 4B 45 59 2D 2D 2D  IN PUBLIC KEY---
```

Sample notification received for a ransomware sample

Now even further meta information is attached to the ransomware sample. For instance, the country from where the sample was uploaded, which might be used to track down the exact location of the victim if it is a branch of an enterprise operating in many countries.

And finally, at some point, you will contract an incident responder because it is very likely that your in-house capabilities won’t be enough. If you tell them that you’ve just uploaded the sample to some online service, chances are that they will not be amused. I’ve never come along an incident responder that was happy when their client uploaded a ransomware sample to the Internet…