# Ryuk Ransomware Likely Behind New Orleans Cyberattack

bleepingcomputer.com/news/security/ryuk-ransomware-likely-behind-new-orleans-cyberattack/

Lawrence Abrams

By
Lawrence Abrams

- December 15, 2019
- 03:46 PM
- 3


Based on files uploaded to the VirusTotal scanning service, the ransomware attack on the City of New Orleans was likely done by the Ryuk Ransomware threat actors.

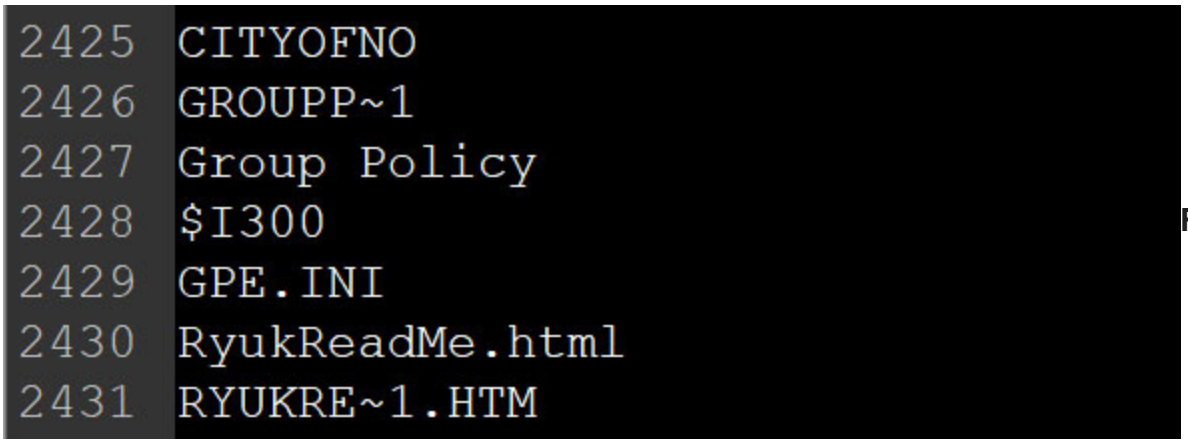
On December 14th, 2019, one day after the City of New Orleans ransomware attack, what appear to be memory dumps of suspicious executables were uploaded from an IP address from the USA to the VirusTotal scanning service.

One of these memory dumps, which contained numerous references to New Orleans and Ryuk, was later found by Colin Cowie of Red Flare Security and shared with BleepingComputer.com.


As memory dumps are a snapshot of the memory being used by an application while it is running, it can be used to extract useful strings, file names, commands, and other information that the executable interacted with or executed. This allows memory dumps to be used during cyber attack forensic investigations to learn more about how the attack was conducted.

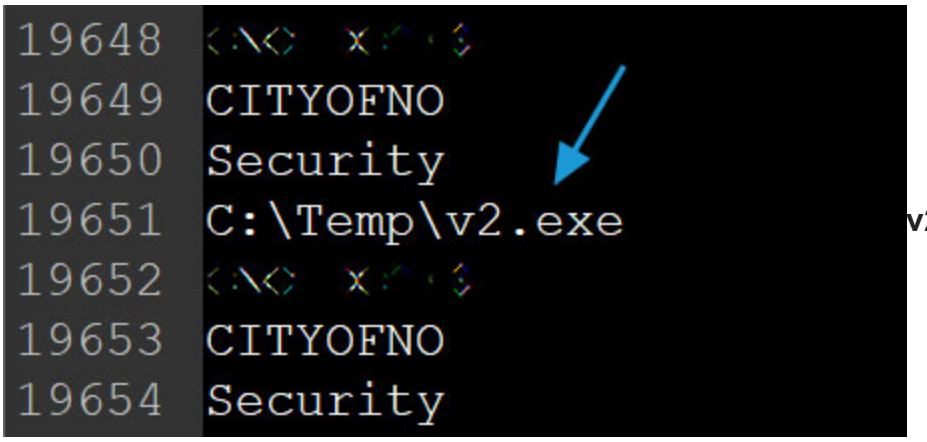
The memory dump found by Cowie is for an executable named 'yoletby.exe' and contains numerous references to the City of New Orleans including domain names, domain controllers, internal IP addresses, user names, file shares, and references to the Ryuk ransomware.

The Ryuk ransomware strings included in the dump were the HERMES file marker, file names ending with the .ryk extension, and references to the created RyukReadMe.html ransom notes.




**Ryuk and City of New Orleans strings**

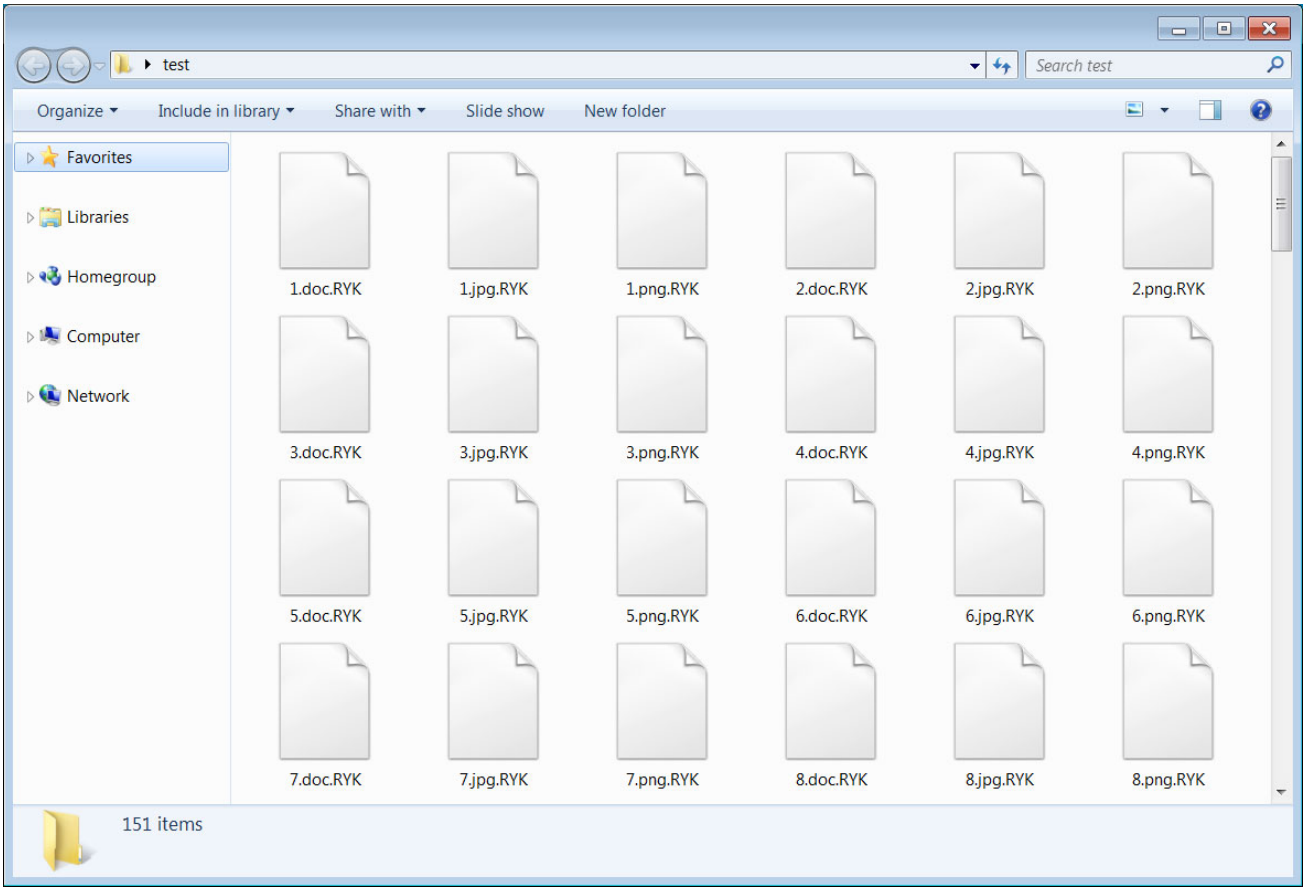
After investigating the file further, BleepingComputer found an interesting reference to the C:\Temp\v2.exe executable that was executed on the machine. It turns out that a memory dump for this file was also uploaded to VirusTotal.




**v2.exe strings**

Of particular interest in the v2.exe memory dump is a string that refers to the New Orleans City Hall.

After further digging around, BleepingComputer was able to find a v2.exe executable, and after executing it, was able to confirm that it was the Ryuk ransomware.




**Files encrypted by Ryuk after executing v2.exe**

While it is not known if this executable is the one used in the City of New Orleans attack, it does show that this filename is used in Ryuk attacks and the memory dumps show that a file of that name was used on an attack against the City of New Orleans.

If the City of New Orleans was indeed encrypted by Ryuk, which by the evidence seems likely, then this is just another victim of Ryuk who has seen increased activity lately.

BleepingComputer has contacted the City of New Orleans for confirmation that they were infected with Ryuk, but have not heard back at this time.

## Emotet and Trickbot likely present as well

If New Orleans was encrypted by Ryuk, there is also a very high chance that the Emotet and TrickBot infections are present on the network as well

Emotet is a malware infection that is commonly spread through spam emails that contain malicious attachments. When opened and macros enabled, these attachments will install the Emotet Trojan on the victim's computer.

Emotet will then use that infected computer to spam other computers with malicious attachments and also download further malware on the computer.

One of the most common malware installed by Emotet is the TrickBot information-stealing Trojan.

When executed, TrickBot will connect back to a command and control server where it will receive commands to load various modules that steal information from the computer or install even further malware.

After the TrickBot actors collect all valuable information and data from the computer, it will then open a reverse shell back to the Ryuk actors.

From there, the Ryuk team will perform reconnaissance of the network, collect admin passwords, take over domain controllers, and utilize post-exploitation toolkits such as PowerShell Empire.

This is why all network admins need to realize that if they have been encrypted by Ryuk, there has commonly been a malware presence on their network for quite a while and that other data may have been stolen or compromised.

## What does this mean for the City of New Orleans?

It means that in addition to the Ryuk Ransomware infection, they also have to deal with the fact that attackers have been snooping around their data for some time.

The city will need to be more diligent against targeted phishing attacks, tighten security on their network, and change passwords.

Also, as it is unknown what financial information may have been attained by the attackers, the City of New Orleans should contact their banking partners and put new procedures in place regarding how money is transferred.

**Update 12/15/19:** Updated article to include how Emotet and Trickbot are usually found with Ryuk infections. Thx @vagab0ndsec and @QW5kcmV3.

### Related Articles:

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

- New Orleans

- Ransomware
- Ryuk

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

## Comments

- 

mrpaddy35 - 2 years ago
  - 
  - 

  Hello i want to know if this is actually caused by Ryuk or also how did you even analyze it ?
  Also those dumps you used to analyze belongs to the victim computer of new oreleans ?

- 

  woody188 - 2 years ago

  - 
  - 

  Files uploaded to VirusTotal are shared with all users unless they are marked private by the uploader. This allows many security researchers to download and analyze actual malware in the wild. Many times these uploads contain indications of their origin. The ones in the article appear to contain domain information that indicate the origin of the files was New Orleans.

- 

  Lawrence Abrams - 2 years ago

  - 
  - 

  Yes, the memory dumps clearly indicate that the processes were running on the City of New Orleans domain

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

## You may also like: