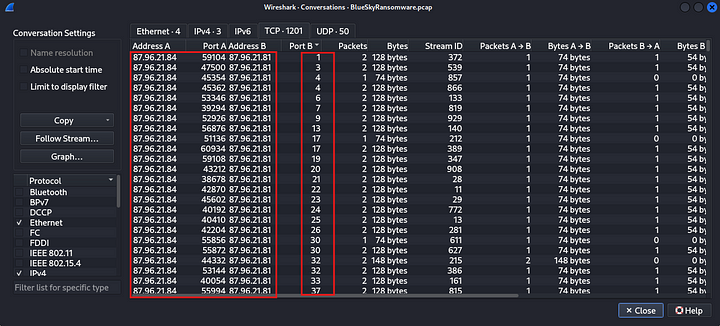
### **BlueSky Ransomware — CyberDefenders**

Scenario: A high-profile corporation that manages critical data and services across diverse industries has reported a significant security incident. Recently, their network has been impacted by a suspected ransomware attack. Key files have been encrypted, causing disruptions and raising concerns about potential data compromise. Early signs point to the involvement of a sophisticated threat actor. Your task is to analyze the evidence provided to uncover the attacker’s methods, assess the extent of the breach, and aid in containing the threat to restore the network’s integrity.

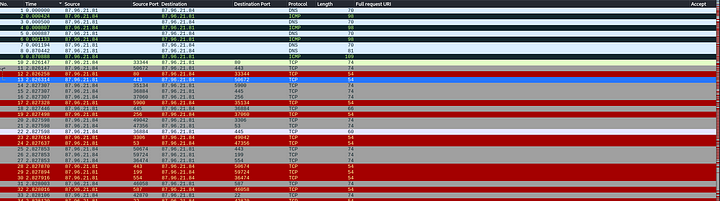
Tasks

1. **Knowing the source IP of the attack allows security teams to respond to potential threats quickly. Can you identify the source IP responsible for potential port scanning activity?**

Let us check the conversations , specifically the TCP tab for any suspicious behavior.



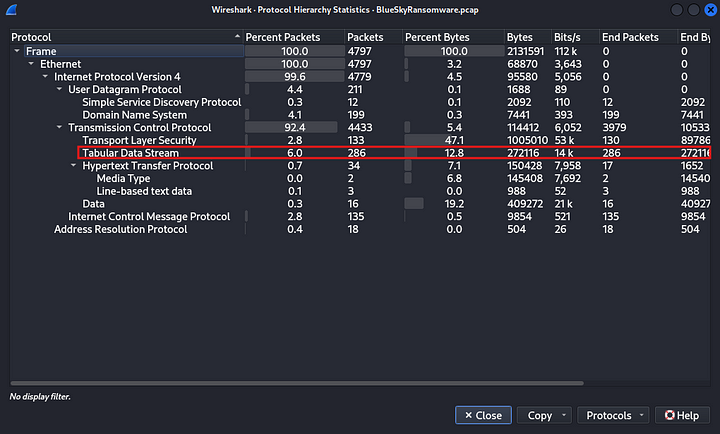
We can see above that 87[.]96[.]21[.]84 is trying to scan for open ports on 87[.]96[.]21[.]81. Also we can see the packets which indicate a syn scan activity.



**Answer:** 87.96.21.84

**2. During the investigation, it’s essential to determine the account targeted by the attacker. Can you identify the targeted account username?**

If we see the protocol hierarchy we can notice that TDS protocol is used inside this capture. Tabular Data Stream (TDS) is an application-level protocol used to transmit data between a database server and a client.



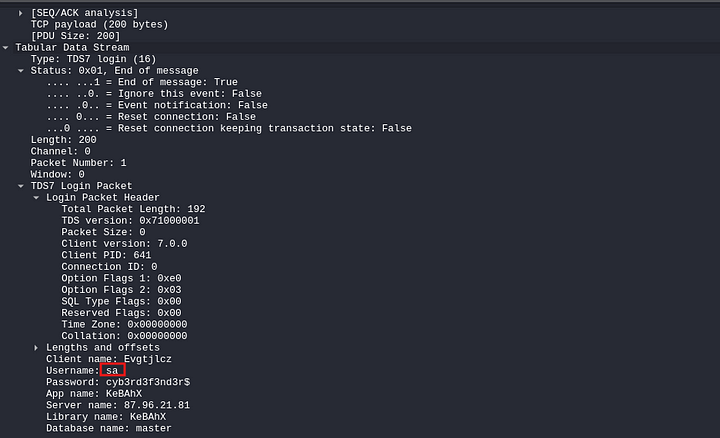
Let us check specifically for the TDS login packet.

Filter: tds.type ==16

This will show the packets sending the login information.



We can see above that we got two packets from this search. Let us check the details of these packets to find the credentials used to login.



**Answer:** sa

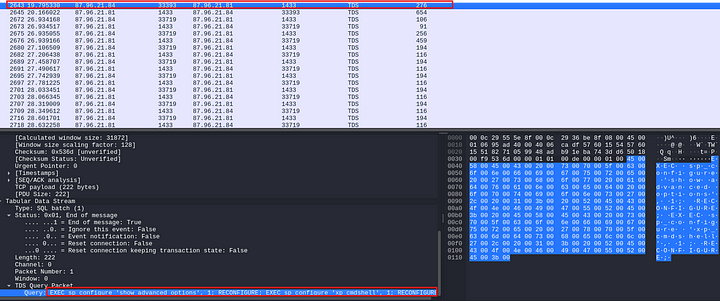
**3. We need to determine if the attacker succeeded in gaining access. Can you provide the correct password discovered by the attacker?**

This can be seen in the above screenshot.

**Answer:** cyb3rd3f3nd3r$

**4. Attackers often change some settings to facilitate lateral movement within a network. What setting did the attacker enable to control the target host further and execute further commands?**

Let us check the TDS packets, after the login packets to see what exactly did the attacker execute.



We cane see above, the malicious command used by the attacker. Now let us understand this command.

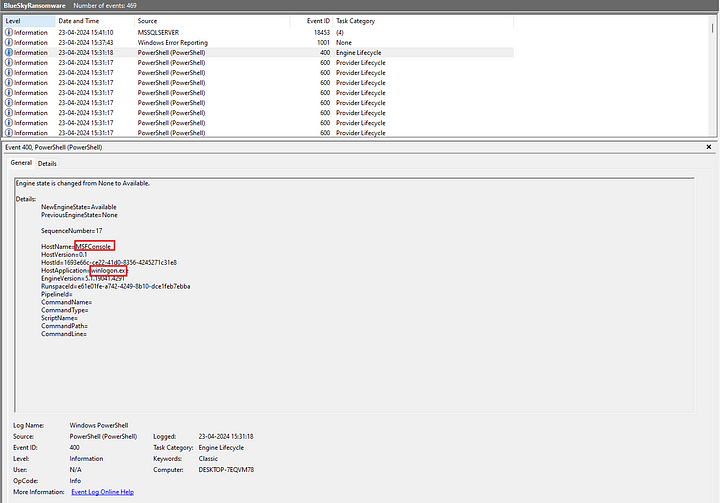


In the above command, the attacker is changing the configuration settings of the SQlserver. Then they are enabling xp\_cmdshell feature. This feature will allow SQL server to run system commands.

**Answer:** xp\_cmdshell

**5. Process injection is often used by attackers to escalate privileges within a system. What process did the attacker inject the C2 into to gain administrative privileges?**

Let us examine the event log file provided for investigation. After opening the log file if we check the third event we can see that HostName=MSFConsole and HostApplication=winlogon.exe.

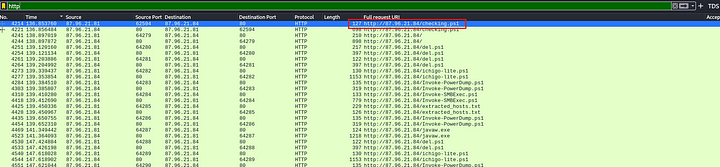


MSFConsole is a command line tool used with Metasploit, a widely used penetration testing framework. winlogon.exe is a system process used to manage user authentication. Modifying this process would give the attacker elevated privileges, potetially giving the attacker full control of the system

**Answer:** winlogon.exe

**6. Following privilege escalation, the attacker attempted to download a file. Can you identify the URL of this file downloaded?**

Let us check the http traffic for any file downloads.

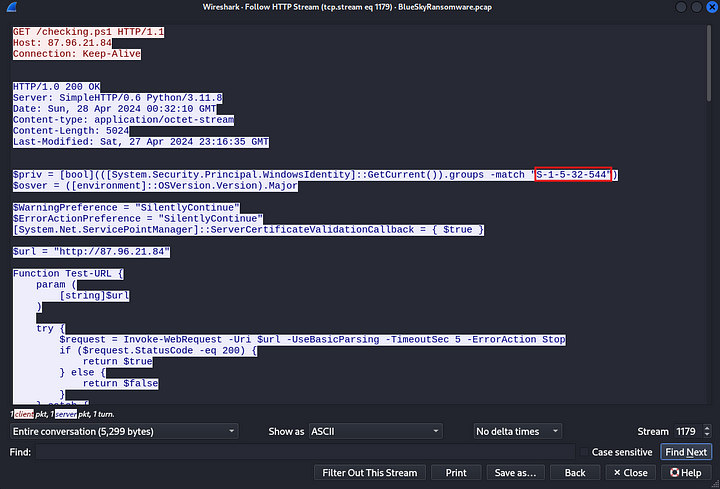


We can see above the file being downloaded from the attacker machine.

**Answer:** http://87[.]96[.]21[.]84/checking.ps1

**7. Understanding which group Security Identifier (SID) the malicious script checks to verify the current user’s privileges can provide insights into the attacker’s intentions. Can you provide the specific Group SID that is being checked?**

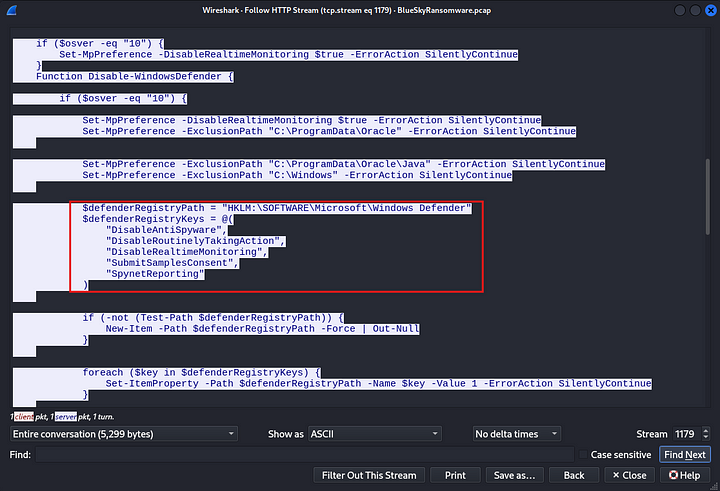
Let us examine the code for the above file to find this. Select the above packet and follow http stream.



**Answer:** S-1–5–32–544

**8. Windows Defender plays a critical role in defending against cyber threats. If an attacker disables it, the system becomes more vulnerable to further attacks. What are the registry keys used by the attacker to disable Windows Defender functionalities? Provide them in the same order found.**

If we scroll down on the same stream, we can see more code from the downloaded powershell script. Somewhere in the middle there is a code to disable the defensive capabilities of Microsoft Defender.

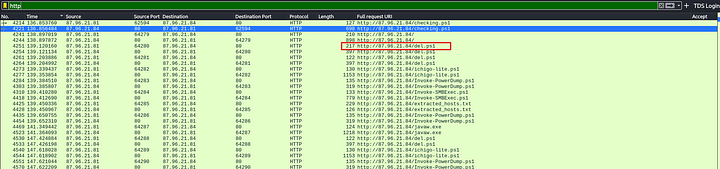


**Answer:** DisableAntiSpyware, DisableRoutinelyTakingAction, DisableRealtimeMonitoring, SubmitSamplesConsent, SpynetReporting

**9. Can you determine the URL of the second file downloaded by the attacker?**

Let us go back to the http packets.

filter: http

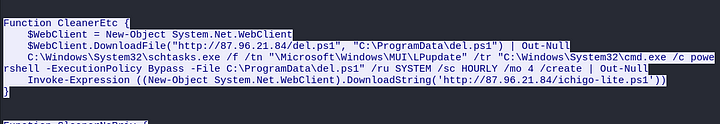


We can see above, the next file downloaded by the attacker.

**Answer:** del.ps1

**10. Identifying malicious tasks and understanding how they were used for persistence helps in fortifying defenses against future attacks. What’s the full name of the task created by the attacker to maintain persistence?**

Let us further examine the code in file 1.

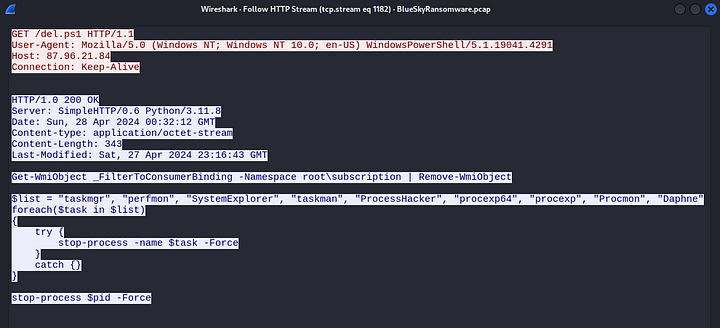


In the above snippet of code, the attacker is trying top download the file called del.ps1 and the creating a process under \Microsoft\Windows\MUI\LPUpdate and scheduling it to run as system every 4 hours with the help of schtasks.exe which is a task scheduler. This will give the attacker, persistent access to the system

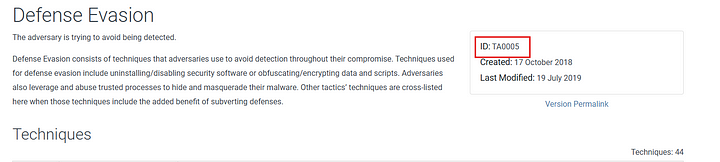
**Answer:** \Microsoft\Windows\MUI\LPUpdate

**11. Based on your analysis of the second malicious file, What is the MITRE ID of the main tactic the second file tries to accomplish?**

Let us check the code inside the second file



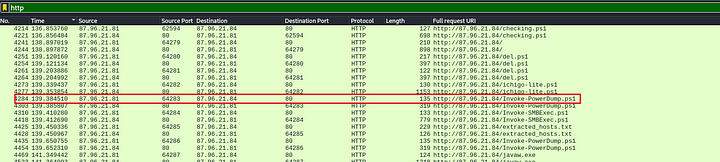
The above code is stopping all the defensive processes on the system. This is used to evade defenses. The tactic associated with this is called Defense Evasion.



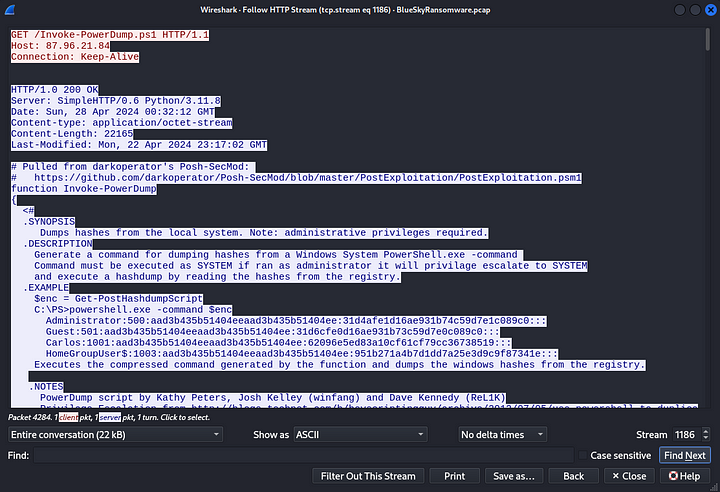
**Answer:** TA0005

**12. What’s the invoked PowerShell script used by the attacker for dumping credentials?**

Let us go back to the http packets.



We can see above a file called Invoke-PowerDump.ps1. Let us examine the code in this file.

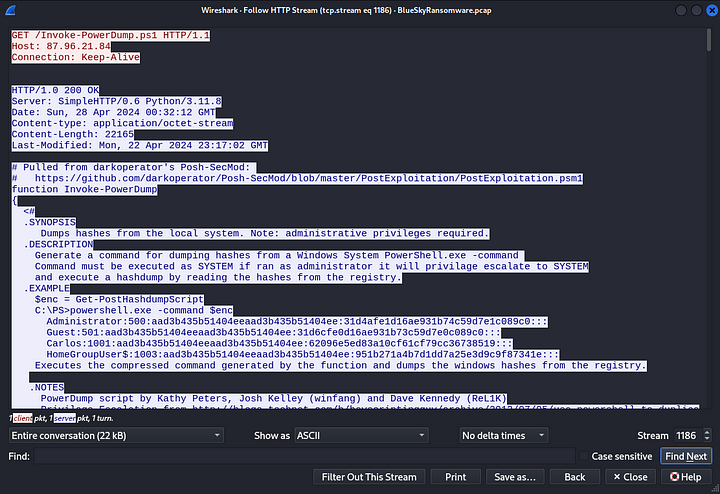


From the synopsis, it is clear that this file is used to extract the hashsed from the system

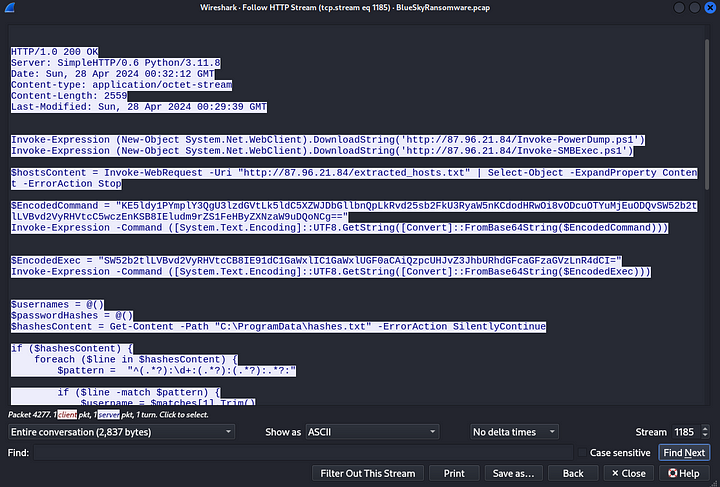
**Answer:** Invoke-PowerDump.ps1

**13. Understanding which credentials have been compromised is essential for assessing the extent of the data breach. What’s the name of the saved text file containing the dumped credentials?**

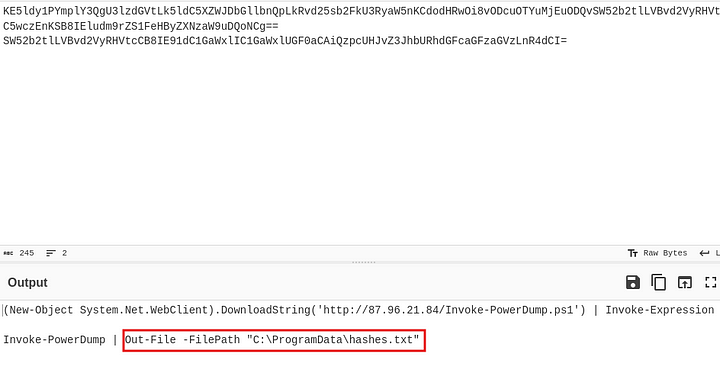
Let us check the code of this file to see if it is creating a file to store the hashes locally.



Seems like this code does not create any file locally. But, the file which was downloaded before this “ichigo-lite.ps1” has some encoded commands and under them there is a path to a file “C:\ProgramData\hashes.txt”



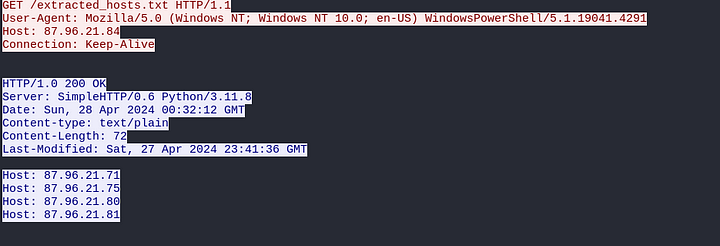
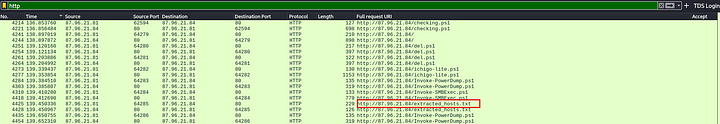
Let us copy the encoded commands and paste in Cyberchef to decode these.



**Answer:** hashes.txt

**14. Knowing the hosts targeted during the attacker’s reconnaissance phase, the security team can prioritize their remediation efforts on these specific hosts. What’s the name of the text file containing the discovered hosts?**

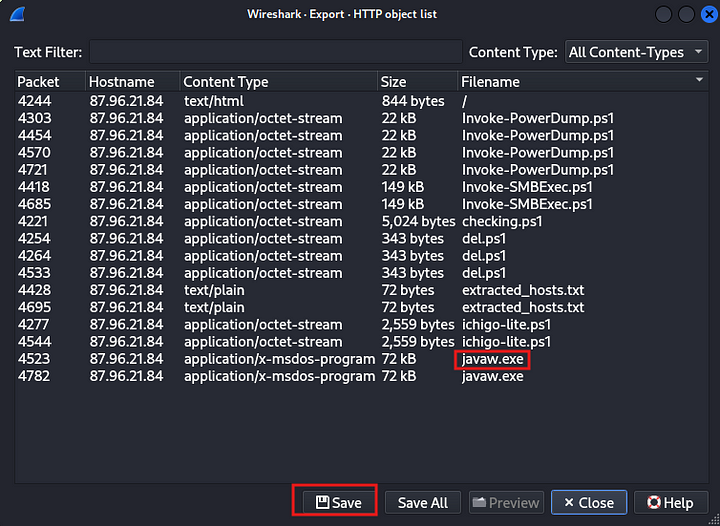
We can find this in the http packets.



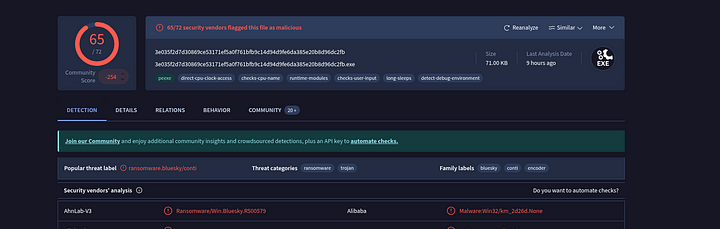
**Answer:** extracted\_hosts.txt

**15. After hash dumping, the attacker attempted to deploy ransomware on the compromised host, spreading it to the rest of the network through previous lateral movement activities using SMB. You’re provided with the ransomware sample for further analysis. By performing behavioral analysis, what’s the name of the ransom note file?**

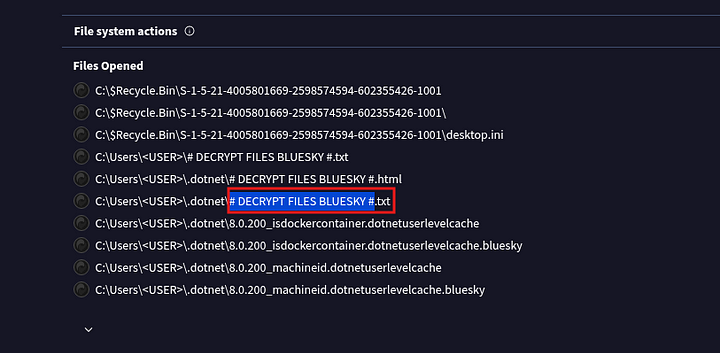
Let us export the ransomware file and examine it(should be done only in an isolated environment)to find out its behaviour.



Calculate the hash of this file and upload it to Virustotal.

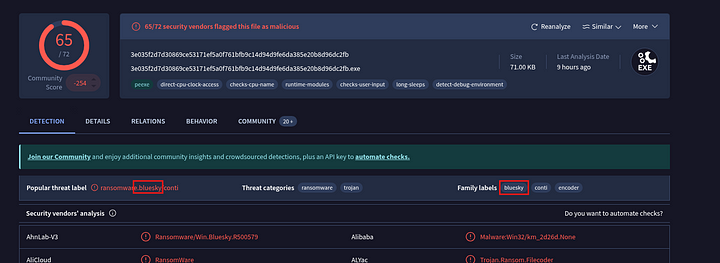


Now, go to the behavior tab and scroll down to the file system actions section. There we can find the file it creates after encryption.



**Answer:** # DECRYPT FILES BLUESKY#

**16. In some cases, decryption tools are available for specific ransomware families. Identifying the family name can lead to a potential decryption solution. What’s the name of this ransomware family?**

****

**Answer:** bluesky

This is the end of this walkthrough.