Volt Typhoon: Part 2 — Leveraging ExoneraTor to Unmask the Threat Actor

Owaiz Khan ⁝⁝ 10/15/2024

Owaiz Khan

ExoneraTor is a service provided by The Tor Project that helps determine whether a specific IP address was part of the Tor network on a given date. It serves as a valuable tool for law enforcement agencies and individuals who need to verify the association of an IP address with Tor activity.

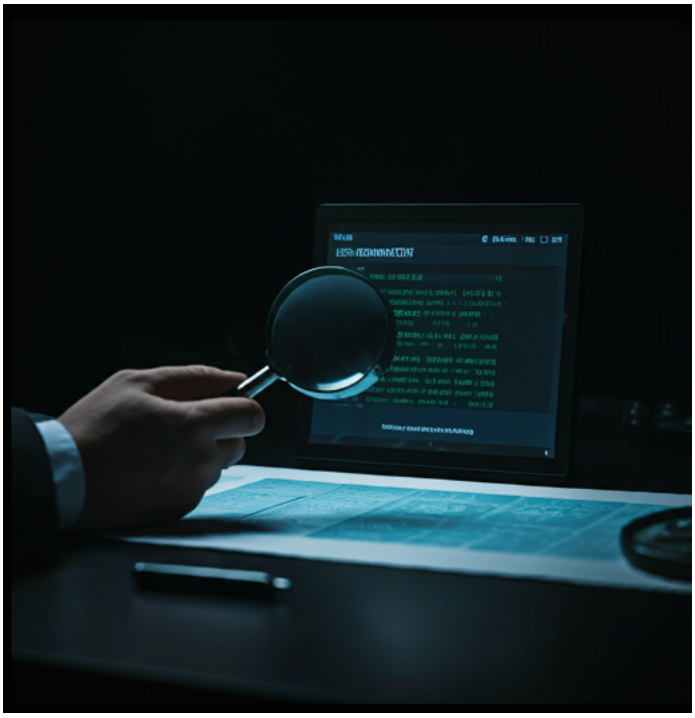


Image taken from Gemini AI

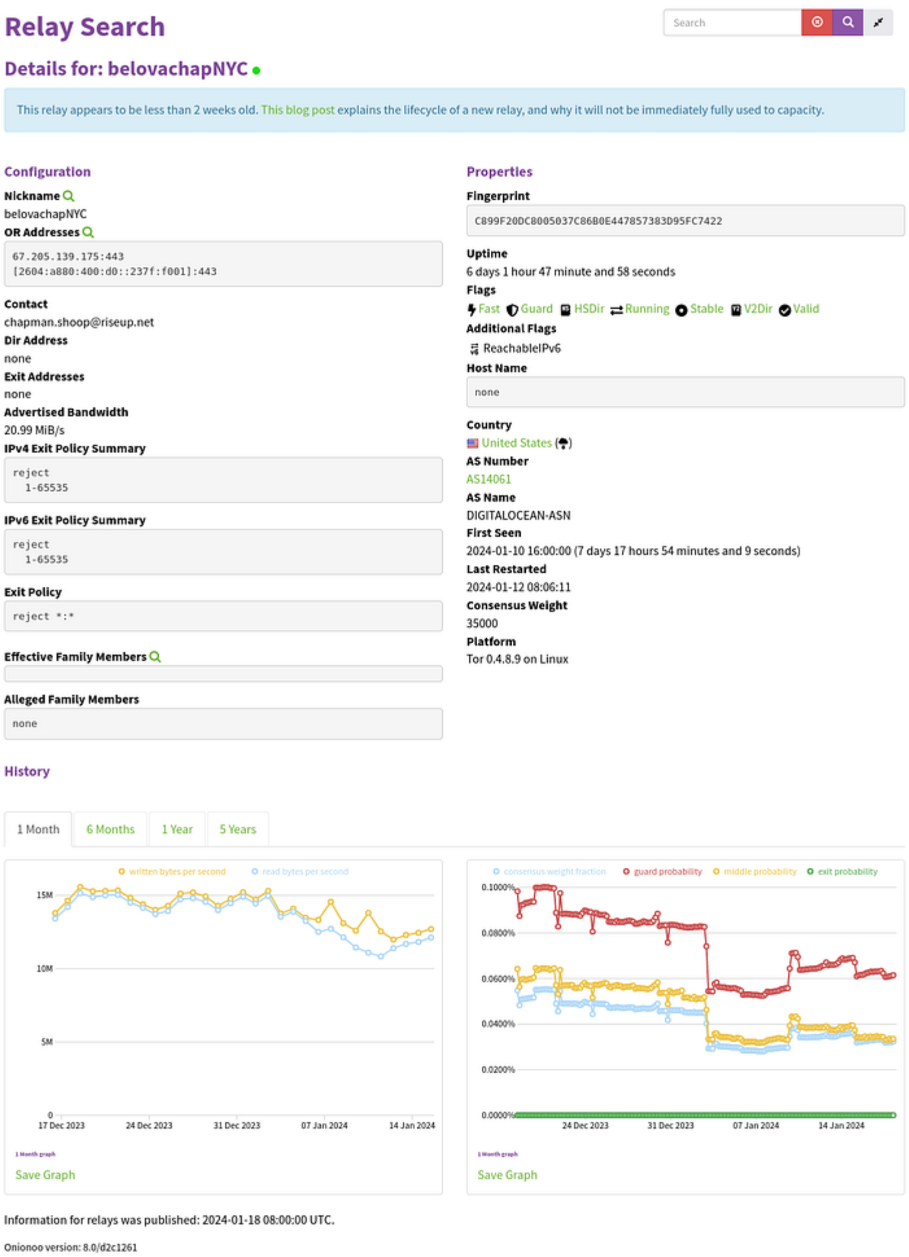
ExoneraTor is a tool provided by The Tor Project that helps determine whether a specific IP address was part of the Tor network on a given date. It can be used in investigations to:

1. If an IP address is suspected of being involved in Tor-related activities, ExoneraTor can confirm or deny its association with the Tor network.
2. It can help track the movement and configuration of Tor relays over time, providing insights into the network's infrastructure.
3. ExoneraTor can be used to investigate cases where online anonymity is suspected to be involved, such as criminal activities or whistleblower disclosures.
4. It can be a valuable tool in digital forensics investigations, helping to identify and analyze Tor-related artifacts.

By providing information about the historical association of IP addresses with the Tor network, ExoneraTor can assist in various investigations and help shed light on online activities that may involve the use of Tor.

Let's use an example to identify a Tor IP address.

According to The Tor Project's ExoneraTor tool, the IP address (example ip = **67.205.139.175**) was not functioning as a Tor exit relay between December 28 and 30, 2023. However, during this time, it was operating as a different type of Tor relay with the fingerprint **C899F20DC8005037C86B0E447857383D95FC7422**. You can find more details about this relay's configuration by searching for its fingerprint on the Tor Metrics portal.



Relay Search

Search

Details for: belovachapNYC ●

This relay appears to be less than 2 weeks old. This blog post explains the lifecycle of a new relay, and why it will not be immediately fully used to capacity.

Configuration

Nickname
belovachapNYC

OR Addresses

```
67.205.139.175:443
[2604:a880:400:d0::237f:f001]:443
```

Contact
chapman.shoop@riseup.net

Dir Address
none

Exit Addresses
none

Advertised Bandwidth
20.99 MiB/s

IPv4 Exit Policy Summary

```
reject
  1-65535
```

IPv6 Exit Policy Summary

```
reject
  1-65535
```

Exit Policy

```
reject *:*
```

Effective Family Members

Alleged Family Members

```
none
```

Properties

Fingerprint

```
C899F20DC8005037C86B0E447857383D95FC7422
```

Uptime
6 days 1 hour 47 minute and 58 seconds

Flags
Fast Guard HSDir Running Stable V2Dir Valid

Additional Flags
ReachableIPv6

Host Name

```
none
```

Country
United States

AS Number
AS14061

AS Name
DIGITALOCEAN-ASN

First Seen
2024-01-10 16:00:00 (7 days 17 hours 54 minutes and 9 seconds)

Last Restarted
2024-01-12 08:06:11

Consensus Weight
35000

Platform
Tor 0.4.8.9 on Linux

History

1 Month | 6 Months | 1 Year | 5 Years

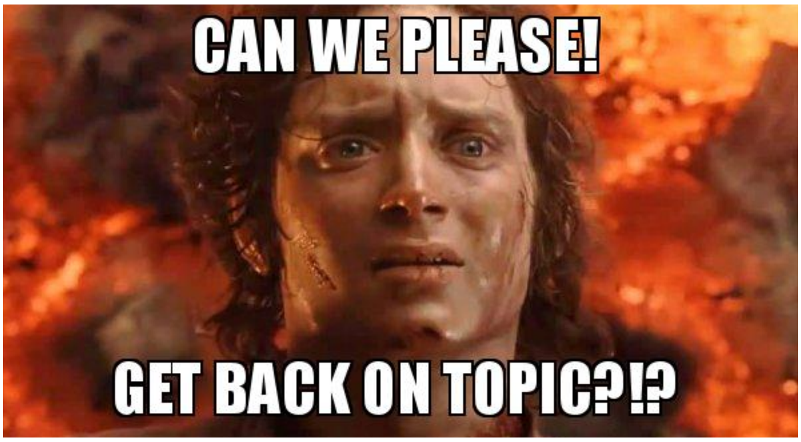
Information for relays was published: 2024-01-18 08:00:00 UTC.

Onionoo version: 8.0/d2c1261

About Volt Typhoon:

Volt Typhoon is a state-sponsored cyber espionage group that has been active since at least 2021, and is believed to be affiliated with the Chinese government

Volt Typhoon is known to primarily target the United States and the manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors. Volt Typhoon focuses on espionage, data theft, and credential access.



Lets not deviate from Topic.

The IP address which we took as an example belongs to a Threat Actor **"VOLT TYPHOON".**

Anyways we are halfway on to the investigation.

Interestingly, Tor Metrics indicates that the Tor relay with fingerprint C899F20DC8005037C86B0E447857383D95FC7422 first appeared on January 10, 2024. This conflicts with Security Scorecard's report.

DCSO believes this discrepancy may be due to a bug in Tor Metrics. ExoneraTor confirms a live Tor relay with the same fingerprint at the same IP address in December 2023. Additionally, historical traffic data shows continuous activity dating back to at least August 31, 2022.

However, it seems the relay was never configured as a Tor exit node. This means standard Tor clients wouldn't have used it to route traffic to the regular internet. Furthermore, the relay's configuration explicitly rejects such connections. DCSO's analysis of raw Tor network data supports this conclusion.

If 67.205.139.175 didn't host a Tor exit node, Volt Typhoon may not have used Tor's internet connectivity features. This could mean they didn't attempt to hide their source IP while performing administrative tasks. The exact implications of this finding are uncertain and require further investigation.

Hypothesis A: 45.63.60.39 is Using or Connecting to a Hidden Service

DCSO initially theorized that 45.63.60.39 might be operating a Hidden Service or frequently connecting to one. In this scenario, 67.205.139.175 could have been one of 45.63.60.39's Entry Guards.

Tor relays must meet specific criteria to become Entry Guards, including stability, bandwidth, and uptime. C899F20DC8005037C86B0E447857383D95FC7422 meets these requirements and is flagged as a Guard, making it eligible for use by Tor clients. In December 2023, there was a 0.08% to 0.1% chance of a random Tor client choosing C899F20DC8005037C86B0E447857383D95FC7422 as an Entry Guard.

If Hypothesis A is correct, Volt Typhoon might be managing some of its command-and-control (C2) infrastructure through a Hidden Service. This aligns with previous reports on their tactics.

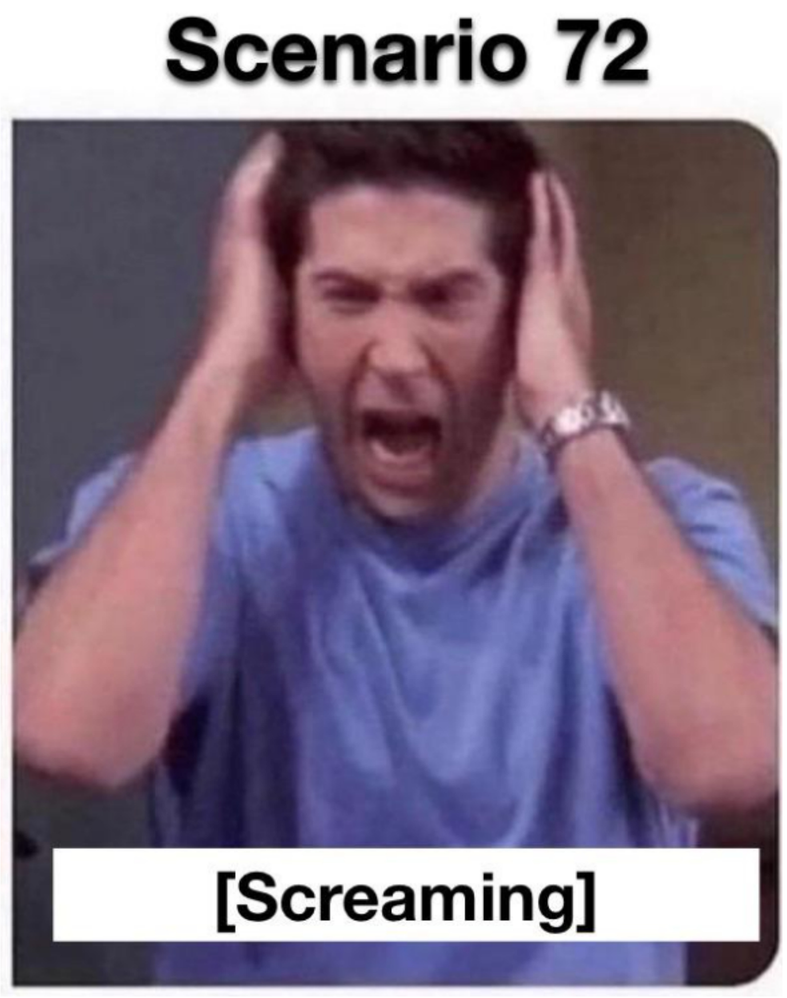
Hidden Services offer benefits, such as keeping traffic within the Tor network and making applications harder to attack. For example, the Terrapin attack against SSH is ineffective when SSH is used with Hidden Services.

However, Hidden Services also have drawbacks, including lower bandwidth, higher latency, and reliance on multiple Tor relays. These factors can make interactive applications like SSH less efficient.

Superficial investigations might dismiss network communication involving Tor relays. Such connections often originate from Tor traffic and can be difficult to trace.

The Tor Project's FAQ mentions that running your own Tor relay can increase resilience against certain traffic correlation attacks. This is because an adversary may struggle to determine if a connection comes from the relay itself or from a Tor user on the same network.

Hypothesis B: Volt Typhoon is Running Tor Relays as a Disguise



However, Tor Hidden Services have several downsides, including lower bandwidth, higher latency, and reliance on the reliability of all Tor relays used for a connection (the “circuit” in Tor jargon). For interactive applications like SSH, the high latency can make usage cumbersome.

Superficial investigations might dismiss network communication involving Tor relays. Such connections often originate from Tor traffic and can be difficult to trace.

The Tor Project’s FAQ mentions that running your own Tor relay can increase resilience against certain traffic correlation attacks. This is because an adversary may struggle to determine if a connection comes from the relay itself or from a Tor user on the same network.

For example, an attacker with control over a few Tor relays might see a connection from you but be unable to determine if it originated from your computer or was relayed by someone else.

The specific attacks you’re concerned about play a significant role. For most users, running a relay is still a good idea.

This works best with Tor exit relays but isn’t foolproof, especially for investigators with access to comprehensive network data.

Conclusion

Based on the ExoneraTor results and the Tor network consensus data analyzed, it seems unlikely that 67.205.139.175 was used by Volt Typhoon as a Tor exit relay to obfuscate the origin of connections to the C2 server located at 45.63.60.39.

However, even if this initial assessment is correct, more information is needed to definitively confirm or rule out either Hypothesis A or B. This includes details like port numbers and traffic metadata.

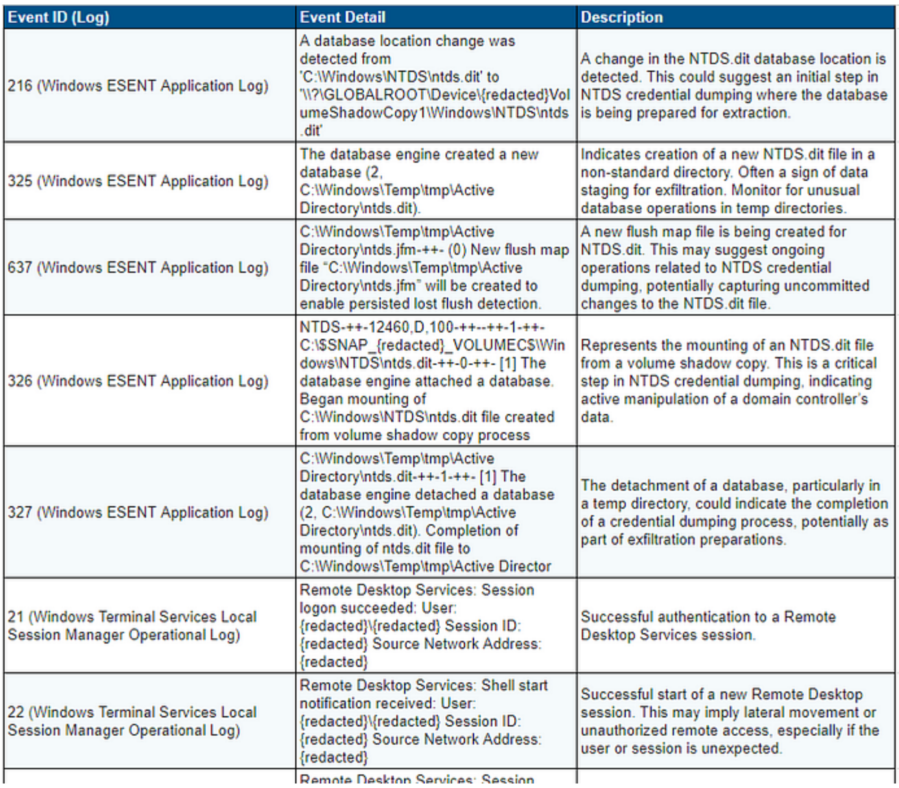
Detecting and Hunting scenarios:

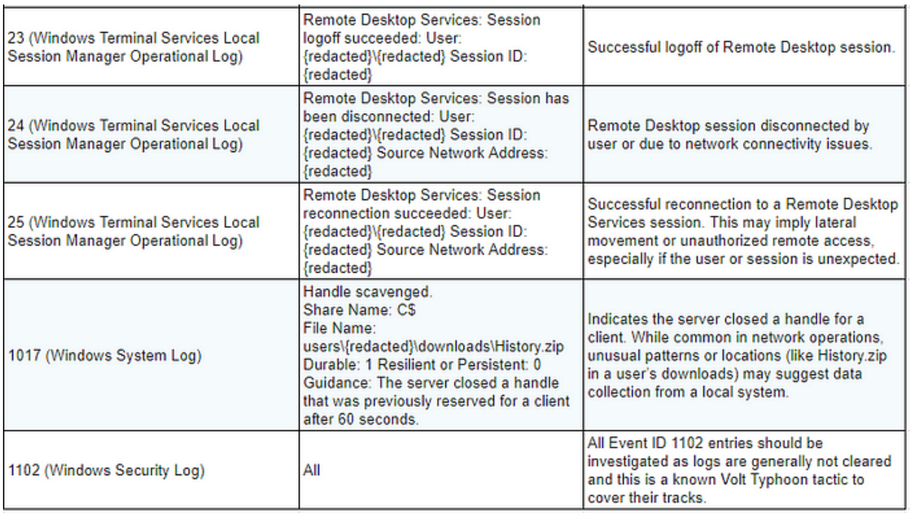
Implement Effective Living off the Land (LOTL) Detection Strategies

To enhance LOTL threat detection, prioritize implementing the recommendations outlined in the joint guide “Identifying and Mitigating Living off the Land Techniques.” Many organizations struggle with LOTL detection due to inadequate security practices and a lack of established baselines. This makes it challenging to differentiate between legitimate and malicious behavior, hindering effective behavior analytics, anomaly detection, and proactive hunting.

Traditional IOCs often fall short in identifying LOTL attacks, complicating detection efforts. This advisory offers a comprehensive cybersecurity strategy incorporating behavior analytics, anomaly detection, and proactive hunting to mitigate LOTL threats effectively.

Check for windows event viewer logs:





Event ID (Log)	Event Detail	Description
216 (Windows ESENT Application Log)	A database location change was detected from 'C:\Windows\NTDS\ntds.dit' to '\\?\GLOBALROOT\Device\{redacted}VolumeShadowCopy1\Windows\NTDS\ntds.dit'	A change in the NTDS.dit database location is detected. This could suggest an initial step in NTDS credential dumping where the database is being prepared for extraction.
325 (Windows ESENT Application Log)	The database engine created a new database (2, C:\Windows\Temp\tmp\Active Directory\ntds.dit).	Indicates creation of a new NTDS.dit file in a non-standard directory. Often a sign of data staging for exfiltration. Monitor for unusual database operations in temp directories.
637 (Windows ESENT Application Log)	C:\Windows\Temp\tmp\Active Directory\ntds.jfm-++- (0) New flush map file "C:\Windows\Temp\tmp\Active Directory\ntds.jfm" will be created to enable persisted lost flush detection.	A new flush map file is being created for NTDS.dit. This may suggest ongoing operations related to NTDS credential dumping, potentially capturing uncommitted changes to the NTDS.dit file.
326 (Windows ESENT Application Log)	NTDS-++-12460,D,100-++--++-1-++-C:\$SNAP_{redacted}_VOLUMEC$\Windows\NTDS\ntds.dit-++-0-++- [1] The database engine attached a database. Began mounting of C:\Windows\NTDS\ntds.dit file created from volume shadow copy process	Represents the mounting of an NTDS.dit file from a volume shadow copy. This is a critical step in NTDS credential dumping, indicating active manipulation of a domain controller's data.
327 (Windows ESENT Application Log)	C:\Windows\Temp\tmp\Active Directory\ntds.dit-++-1-++- [1] The database engine detached a database (2, C:\Windows\Temp\tmp\Active Directory\ntds.dit). Completion of mounting of ntds.dit file to C:\Windows\Temp\tmp\Active Director	The detachment of a database, particularly in a temp directory, could indicate the completion of a credential dumping process, potentially as part of exfiltration preparations.
21 (Windows Terminal Services Local Session Manager Operational Log)	Remote Desktop Services: Session logon succeeded: User: {redacted}\{redacted} Session ID: {redacted} Source Network Address: {redacted}	Successful authentication to a Remote Desktop Services session.
22 (Windows Terminal Services Local Session Manager Operational Log)	Remote Desktop Services: Shell start notification received: User: {redacted}\{redacted} Session ID: {redacted} Source Network Address: {redacted}	Successful start of a new Remote Desktop session. This may imply lateral movement or unauthorized remote access, especially if the user or session is unexpected.
23 (Windows Terminal Services Local Session Manager Operational Log)	Remote Desktop Services: Session logoff succeeded: User: {redacted}\{redacted} Session ID: {redacted}	Successful logoff of Remote Desktop session.
24 (Windows Terminal Services Local Session Manager Operational Log)	Remote Desktop Services: Session has been disconnected: User: {redacted}\{redacted} Session ID: {redacted} Source Network Address: {redacted}	Remote Desktop session disconnected by user or due to network connectivity issues.
25 (Windows Terminal Services Local Session Manager Operational Log)	Remote Desktop Services: Session reconnection succeeded: User: {redacted}\{redacted} Session ID: {redacted} Source Network Address: {redacted}	Successful reconnection to a Remote Desktop Services session. This may imply lateral movement or unauthorized remote access, especially if the user or session is unexpected.
1017 (Windows System Log)	Handle scavenged. Share Name: C$ File Name: users\{redacted}\downloads\History.zip Durable: 1 Resilient or Persistent: 0 Guidance: The server closed a handle that was previously reserved for a client after 60 seconds.	Indicates the server closed a handle for a client. While common in network operations, unusual patterns or locations (like History.zip in a user's downloads) may suggest data collection from a local system.
1102 (Windows Security Log)	All	All Event ID 1102 entries should be investigated as logs are generally not cleared and this is a known Volt Typhoon tactic to cover their tracks.

Key Indicators of Compromise (IOCs) from Recent Cyberattacks

The following indicators of compromise were identified during our investigation. We urge our customers to carefully examine their environments for these IOCs and take immediate action to implement robust detection and protection measures to prevent future attacks and mitigate any potential damage.

Volt Typhoon custom FRP executable (SHA-256):

```
baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231cb4f7c5e3f14fb57be8b5f020377b993618b6e35
```