Threat Modeling Report

Created on 11/10/2019 3:50:21 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

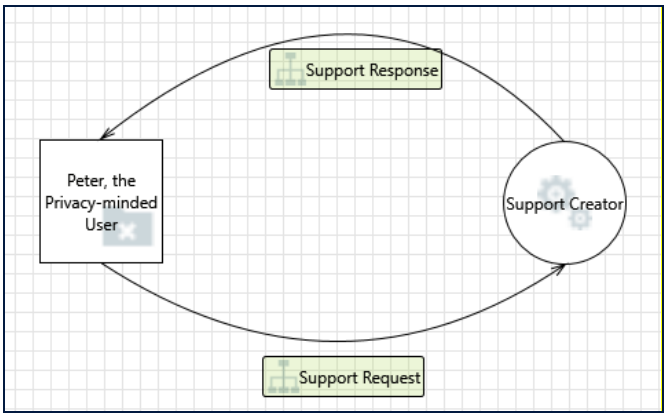
Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	0
Not Applicable	14
Needs Investigation	2
Mitigation Implemented	9
Total	25
Total Migrated	0

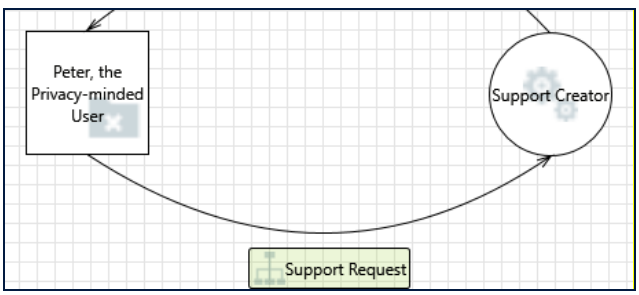
Diagram: Wallet L0



Wallet L0 Diagram Summary:

Not Started	0
Not Applicable	2
Needs Investigation	0
Mitigation Implemented	0
Total	2
Total Migrated	0

Interaction: Support Request



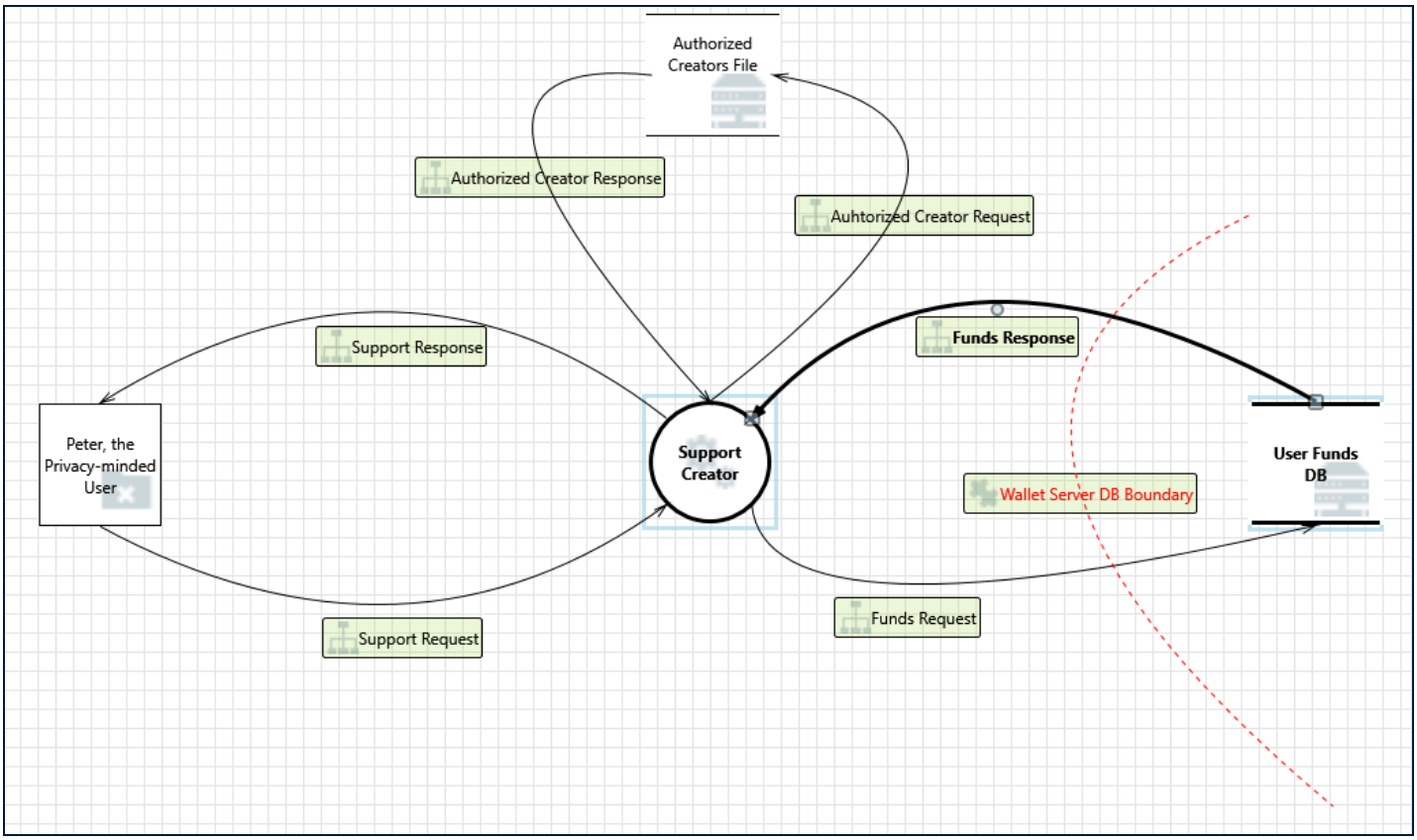
1. Spoofing the Generic External Interactor External Entity [State: Not Applicable] [Priority: High]

Category:	Spoofing
Description:	Peter, the Privacy-minded User may be spoofed by an attacker and this may lead to unauthorized access to Support Creator. Consider using a standard authentication mechanism to identify the external entity.
Justification:	This attack is out of scope. The User will only have access to Supporting Creators that have followed Brave's signup process.

2. Elevation Using Impersonation [State: Not Applicable] [Priority: High]

Category:	Elevation Of Privilege
Description:	Support Creator may be able to impersonate the context of Peter, the Privacy-minded User in order to gain additional privilege.
Justification:	Creators must go through Braves signup process to be considered a Creator. (https://creators.brave.com/)

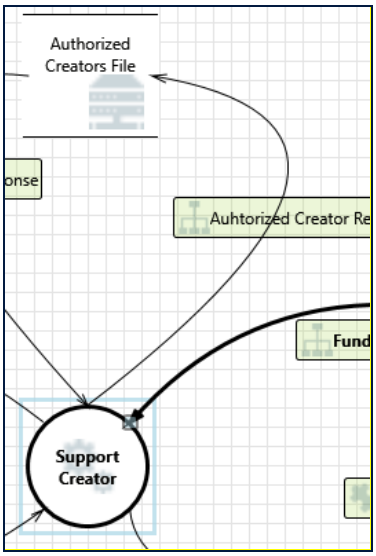
Diagram: Wallet L1



Wallet L1 Diagram Summary:

Not Started	0
Not Applicable	12
Needs Investigation	2
Mitigation Implemented	9
Total	23
Total Migrated	0

Interaction: Auhtorized Creator Request



3. Spoofing of Destination Data Store Authorized Creators File [State: Needs Investigation] [Priority: High]

Category: Spoofing

Description: Authorized Creators File may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Authorized Creators File . Consider using a standard authentication mechanism to identify the destination data store.

Justification: Creators must go through Brave signup process and will only be put on a list for users to choose whether or not they will want to donate to their content. (https://creators.brave.com/) However, after review of signup process, bad actors may still linger.

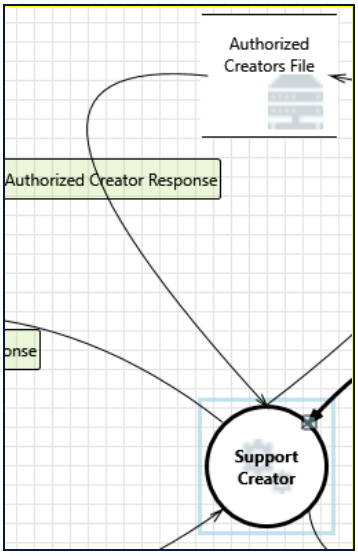
4. Potential Excessive Resource Consumption for Support Creator or Authorized Creators File [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: Does Support Creator or Authorized Creators File take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: This attack is out of scope even though DoS attacks are always possible. DoS attacks are typically not handled by the browser.

Interaction: Authorized Creator Response



5. Weak Access Control for a Resource [State: Not Applicable] [Priority: High]

Category: Information Disclosure

Description: Improper data protection of Authorized Creators File can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: Brave users are able to see the list of valid Creators for them to view and see who they want to support and further donate to. Ex. (https://brave.com/brave-rewards-youtube/)

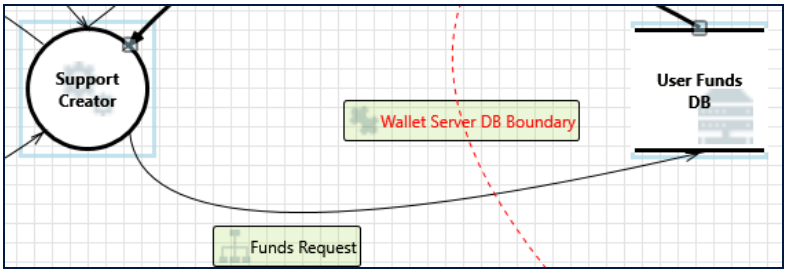
6. Spoofing of Source Data Store Authorized Creators File [State: Not Applicable] [Priority: High]

Category: Spoofing

Description: Authorized Creators File may be spoofed by an attacker and this may lead to incorrect data delivered to Support Creator. Consider using a standard authentication mechanism to identify the source data store.

Justification: The list of Creators is simply a list that is vetted by Brave inorder to allow a Creator to be authorized. (https://creators.brave.com/)

Interaction: Funds Request



7. Potential Excessive Resource Consumption for Support Creator or User Funds DB [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: Does Support Creator or User Funds DB take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: Denial of service attacks of this type are generally not handled by the browser. This attack is something Brave systems would handle.

8. Spoofing of Destination Data Store User Funds DB [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: User Funds DB may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of User Funds DB. Consider using a standard authentication mechanism to identify the destination data store.

Justification: User funds are protected through Uphold's access and encryption process, stoping bad actors from taking advantage of the user and system. (https://support.uphold.com/hc/en-us/articles/203399367-Security-at-Uphold)

9. Spoofing the Support Creator Process [State: Not Applicable] [Priority: High]

Category: Spoofing

Description: Support Creator may be spoofed by an attacker and this may lead to unauthorized access to User Funds DB. Consider using a standard authentication mechanism to identify the source process.

Justification: Brave's partner, Uphold, access and encryption process prevents lateral movement of login access. (https://support.uphold.com/hc/en-us/articles/203399367-Security-at-Uphold)

10. The User Funds DB Data Store Could Be Corrupted [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across Funds Request may be tampered with by an attacker. This may lead to corruption of User Funds DB. Ensure the integrity of the data flow to the data store.

Justification: As mentioned in our SSL DFD (#14), SSL implementations prevent an attacker from decrypting traffic. (Please see SSL DFD - "14. Potential Lack of Input Validation for Browser Process" for more information.)

11. Data Store Denies User Funds DB Potentially Writing Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: User Funds DB claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Uphold's auditing process records traffic allowing for a review to occur if needed. (https://support.uphold.com/hc/en-us/articles/203399367-Security-at-Uphold)

12. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Data flowing across Funds Request may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: As mentioned in our SSL DFD (#14), SSL implementations prevent an attacker from decrypting traffic. (Please see SSL DFD - "14. Potential Lack of Input Validation for Browser Process" for more information.

13. Data Flow Funds Request Is Potentially Interrupted [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: DoS attacks typically aren't handled by the browser. Nevertheless, SSL implementations would prevent an data leakage but Brave and Uphold systems will handle DoS; thus out of scope.

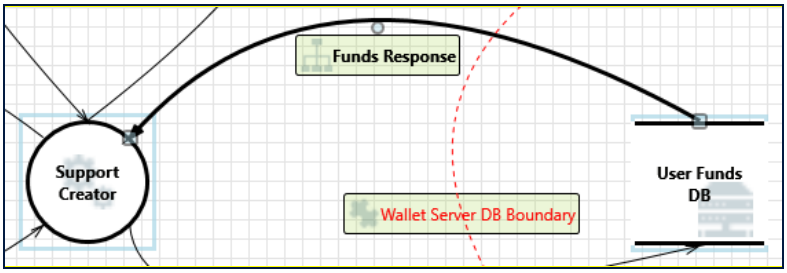
14. Data Store Inaccessible [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: An external agent prevents access to a data store on the other side of the trust boundary.

Justification: DoS attacks typically aren't handled by the browser.

Interaction: Funds Response



15. Spoofing of Source Data Store User Funds DB [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: User Funds DB may be spoofed by an attacker and this may lead to incorrect data delivered to Support Creator. Consider using a standard authentication mechanism to identify the source data store.

Justification: Login authentication and verification prevents an attacker by spoofing this user's funds. (https://uphold.com/en/brave/) However, we can't rule out the idea of this not occuring in today's era. In the past, we have seen many comapnies in the news due to data breaches that occured, which could always be a possiblity; costing users and the company money.

16. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Improper data protection of User Funds DB can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: User funds are protected through Uphold's access and encryption process, stoping bad actors from taking advantage of the user and system. (https://support.uphold.com/hc/en-us/articles/203399367-Security-at-Uphold)

17. Spoofing the Support Creator Process [State: Needs Investigation] [Priority: High]

Category: Spoofing

Description: Support Creator may be spoofed by an attacker and this may lead to information disclosure by User Funds DB. Consider using a standard authentication mechanism to identify the destination process.

Justification: Creators must go through Braves signup process to be considered a Creator. (https://creators.brave.com/) However, an attacker can create an valid Suporter account, that could lead a valid user into donating to a bad actor.

18. Potential Data Repudiation by Support Creator [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Support Creator claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Uphold's auditing logs will prevent any repudiation attacks from a Creator claiming they did not recieve any data. (https://support.uphold.com/hc/en-us/articles/203399367-Security-at-Uphold) Also, Brave's Creator dashboard will log transactions received. (https://creators.brave.com/)

19. Potential Process Crash or Stop for Support Creator [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: Support Creator crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: DoS attacks are not applicable to a Creator's account from crashing. This would be an issue Brave would have to handle in order to keep systems up and running at all times.

20. Data Flow Funds Response Is Potentially Interrupted [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Once again, DoS attacks typically aren't handled by the browser. Nevertheless, SSL implementations would prevent an data leakage but Brave and Uphold systems will handle DoS; thus out of scope

21. Data Store Inaccessible [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: An external agent prevents access to a data store on the other side of the trust boundary.

Justification: Once again, this DoS attack is not applicable to this situation. The user would have to hope that Brave and Uphold systems are up and running at all times in order to prevent a user from not being able to donate or view funds.

22. Support Creator May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: User Funds DB may be able to remotely execute code for Support Creator.

Justification: This attack is not applicable to this situation. A Creator must go through Brave's signup process in order to be verified. User funds are also handled by Brave's partner Uphold, which is another system. Uphold's access and encryption will prevent a Creator from conducting such attack. (https://support.uphold.com/hc/en-us/articles/203399367-Security-at-Uphold)

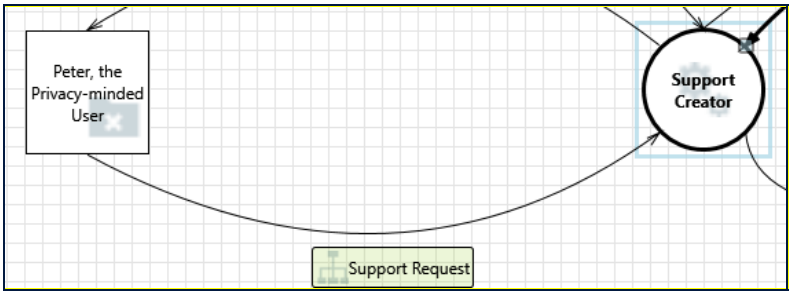
23. Elevation by Changing the Execution Flow in Support Creator [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Support Creator in order to change the flow of program execution within Support Creator to the attacker's choosing.

Justification: As mentioned in our SSL DFD (#14), SSL implementations prevents an attacker from passing manipulated data into Supporting a Creator. (Please see SSL DFD - "14. Potential Lack of Input Validation for Browser Process" for more information.

Interaction: Support Request



24. Spoofing the Peter, the Privacy-minded User External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Peter, the Privacy-minded User may be spoofed by an attacker and this may lead to unauthorized access to Support Creator. Consider using a standard authentication mechanism to identify the external entity.

Justification: Login authentication and verification prevents an attacker by spoofing this user. (https://uphold.com/en/brave/)

25. Elevation Using Impersonation [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: Support Creator may be able to impersonate the context of Peter, the Privacy-minded User in order to gain additional privilege.

Justification: Creators must go through Brave signup process and will only be put on a list for users to choose whether or not they will want to donate to their content. (https://creators.brave.com/)