

Below are the accuracies and losses of the original model, as well as a plot visualization for performance.

```
Epoch number 1
training loss: 0.283 training accuracy: 98.44% || val. loss: 0.067 val. accuracy: 96.88%
Epoch number 2
training loss: 0.066 training accuracy: 99.22% || val. loss: 0.053 val. accuracy: 98.24%
Epoch number 3
training loss: 0.048 training accuracy: 99.22% || val. loss: 0.054 val. accuracy: 98.24%
Epoch number 4
training loss: 0.037 training accuracy: 99.22% || val. loss: 0.055 val. accuracy: 98.63%
Epoch number 5
training loss: 0.033 training accuracy: 100.00% || val. loss: 0.039 val. accuracy: 99.02%
Epoch number 6
training loss: 0.031 training accuracy: 100.00% || val. loss: 0.047 val. accuracy: 98.24%
Epoch number 7
training loss: 0.023 training accuracy: 100.00% || val. loss: 0.047 val. accuracy: 99.02%
Epoch number 8
training loss: 0.023 training accuracy: 100.00% || val. loss: 0.044 val. accuracy: 98.24%
Epoch number 9
training loss: 0.022 training accuracy: 93.75% || val. loss: 0.064 val. accuracy: 98.05%
Epoch number 10
training loss: 0.023 training accuracy: 99.22% || val. loss: 0.047 val. accuracy: 99.02%
Epoch number 11
training loss: 0.022 training accuracy: 100.00% || val. loss: 0.051 val. accuracy: 99.02%
Epoch number 12
training loss: 0.023 training accuracy: 100.00% || val. loss: 0.060 val. accuracy: 98.63%
Epoch number 13
training loss: 0.023 training accuracy: 99.22% || val. loss: 0.043 val. accuracy: 99.02%
Epoch number 14
training loss: 0.020 training accuracy: 96.88% || val. loss: 0.058 val. accuracy: 98.44%
Epoch number 15
training loss: 0.020 training accuracy: 100.00% || val. loss: 0.059 val. accuracy: 98.83%
Epoch number 16
training loss: 0.019 training accuracy: 100.00% || val. loss: 0.066 val. accuracy: 98.44%
Epoch number 17
training loss: 0.024 training accuracy: 99.22% || val. loss: 0.081 val. accuracy: 98.63%
Epoch number 18
training loss: 0.022 training accuracy: 99.22% || val. loss: 0.091 val. accuracy: 98.44%
Epoch number 19
training loss: 0.023 training accuracy: 100.00% || val. loss: 0.069 val. accuracy: 98.05%
Epoch number 20
training loss: 0.017 training accuracy: 99.22% || val. loss: 0.087 val. accuracy: 97.85%
```



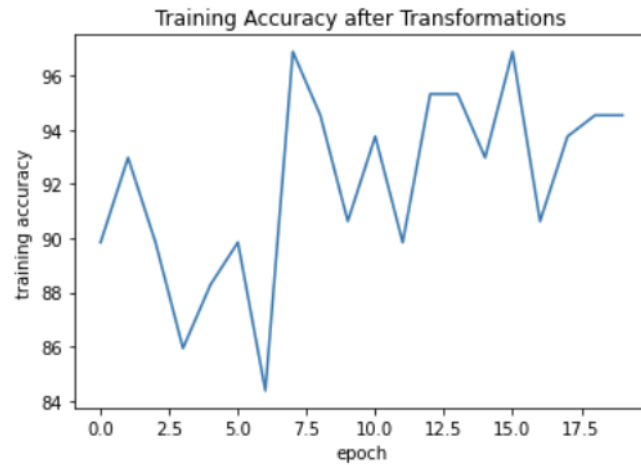
Accuracy of the model on the 10000 test images: 97.72 %

The accuracy of the original model after the adversarial attack decreased by 82.97%:

Accuracy of the model on the 10000 test images: 14.75 %

Below are the accuracies and losses of the model with transformed data, as well as a plot visualization for performance.

```
Epoch number 1
training loss: 0.031 training accuracy: 89.84% || val. loss: 1.457 val. accuracy: 89.84%
Epoch number 2
training loss: 0.028 training accuracy: 92.97% || val. loss: 0.853 val. accuracy: 92.97%
Epoch number 3
training loss: 0.026 training accuracy: 89.84% || val. loss: 1.061 val. accuracy: 92.77%
Epoch number 4
training loss: 0.024 training accuracy: 85.94% || val. loss: 1.066 val. accuracy: 91.80%
Epoch number 5
training loss: 0.022 training accuracy: 88.28% || val. loss: 1.308 val. accuracy: 89.65%
Epoch number 6
training loss: 0.021 training accuracy: 89.84% || val. loss: 1.067 val. accuracy: 94.14%
Epoch number 7
training loss: 0.021 training accuracy: 84.38% || val. loss: 1.145 val. accuracy: 92.19%
Epoch number 8
training loss: 0.021 training accuracy: 96.88% || val. loss: 0.607 val. accuracy: 94.14%
Epoch number 9
training loss: 0.018 training accuracy: 94.53% || val. loss: 1.100 val. accuracy: 92.19%
Epoch number 10
training loss: 0.015 training accuracy: 90.62% || val. loss: 0.899 val. accuracy: 92.97%
Epoch number 11
training loss: 0.016 training accuracy: 93.75% || val. loss: 0.539 val. accuracy: 96.09%
Epoch number 12
training loss: 0.020 training accuracy: 89.84% || val. loss: 0.610 val. accuracy: 93.36%
Epoch number 13
training loss: 0.014 training accuracy: 95.31% || val. loss: 0.699 val. accuracy: 94.53%
Epoch number 14
training loss: 0.012 training accuracy: 95.31% || val. loss: 0.428 val. accuracy: 95.70%
Epoch number 15
training loss: 0.015 training accuracy: 92.97% || val. loss: 0.695 val. accuracy: 95.12%
Epoch number 16
training loss: 0.013 training accuracy: 96.88% || val. loss: 0.517 val. accuracy: 96.68%
Epoch number 17
training loss: 0.012 training accuracy: 90.62% || val. loss: 1.220 val. accuracy: 92.77%
Epoch number 18
training loss: 0.010 training accuracy: 93.75% || val. loss: 0.725 val. accuracy: 97.27%
Epoch number 19
training loss: 0.013 training accuracy: 94.53% || val. loss: 0.696 val. accuracy: 94.73%
Epoch number 20
training loss: 0.014 training accuracy: 94.53% || val. loss: 0.374 val. accuracy: 97.46%
```



The accuracy of the model with transformed data after the adversarial attack decreased only by 71.92%:

Accuracy of the model on the 10000 test images: 25.8 %

The transformations resulted in a 11.05% increase in accuracy, which I think is successful! In the future, I could look into more official ways to prevent cybersecurity attacks.