

# **Desktop Goose**

Embry-Riddle Aeronautical University - Prescott, AZ

Brandon Schlabach, Tyler Stiff, Amanda Davenport

CI410: Malware Analysis | Section 02

Dr. Jon Haass

April 28, 2022

## Summary/Abstract

This report was conducted by Team 4 consisting of Brandon Schlabach, Tyler Stiff, and Amanda Davenport for CI410 Sec 02 on Tuesday/Thursday at 1:25. Desktop Goose is an anti-efficiency, anti-productivity virtual pet with mostly non-malicious intentions. Desktop Goose was created by Sam Chiet and later modified by Jesús A. Álvarez to allow users to run Desktop Goose on MacOS. Desktop Goose was released on January 30th, 2020. The only way to completely stop the Goose from affecting your system is to completely remove it from your computer. That does not mean just deleting the file from the computer, as fragments could be left behind in the processes allowing the Goose to get back in. Its constantly running behavior makes this a good program for malicious actors to use as a backdoor for more malicious programs. If allowed to run without monitorization, the goose will overload the computer, causing it to completely crash. A known malicious aspect of the goose are mods that can be downloaded off the internet that are marketed to “enhance the Goose”. Threat actors will hide malicious files within the modifications that include backdoor and trojans, that will look to further affect the users’ system when the mod is downloaded. Malicious mods, such as “Clicker” will give the program access to the mouse allowing it to click and open applications without the user's consent.

# Table of Contents

<b>Summary/Abstract</b>	<b>2</b>
<b>Table of Contents</b>	<b>3</b>
<b>Introduction</b>	<b>4</b>
<b>Methods</b>	<b>4</b>
Setup	4
Tools	4
<b>Findings</b>	<b>5</b>
Identifiers	5
Discoveries	5
Challenges	5
Static Analysis	7
Virus Total	7
Cuckoo Sandbox	7
Interesting Section:	8
Imports	8
Dynamic Analysis	10
Program	10
Resource Monitor	10
Processes with Network Activity	10
CPU	11
Process Tree	11
Fakenet	11
Desktop Goose Dependent Files	12
ANY.RUN	12
<b>Mitigations</b>	<b>13</b>
<b>Conclusion</b>	<b>13</b>
<b>Bibliography</b>	<b>15</b>
<b>Appendix 1 - Associated Files</b>	<b>16</b>

## Introduction

Desktop Goose is considered grayware malware. These types of malware are not referred to as obviously malicious applications and are not classified as a virus, but can still be irritating or even harmful. One such action is sending unwanted pop-ups to your screen, which is the main form of unwanted action used by the Desktop Goose. The Desktop Goose can also grab the user's mouse pointer and move it when the user closes an unwanted pop-up. The major effect of grayware on a target system is depleted computer performance, which could leave the device open to further security risks.

## Methods

### Setup

We downloaded Desktop Goose from [samperson.itch.io/desktop-goose](https://samperson.itch.io/desktop-goose). It downloads an extractor that must be run to extract the folder where the executable is. Once the executable is run, a goose will appear on the desktop and begin walking around.

### Tools

The following is a list of tools used during the analysis of GooseDesktop.exe.

Tool Name	Version
Cuckoo Sandbox	5.4.0.70-generic
Ghidra	9.2.2
IDA Freeware	7.0
Virus Total	API 3
Windows 7 Professional	6.1.7601 Service Pack 1 Build 7601

## Findings

### Identifiers

File:	GooseDesktop.exe
File Type:	Win32 EXE
Version:	1.0.0.0
MD5:	C883E2C769EBE56240A71260B17F1B93
SHA-256:	943FD1EA44266C5D7FA02F2B292DB095A4E6BA8027A1F6C73FD60D11 65E63AFF
ImpHash:	F34D5F2D4577ED6D9CEEC516C1F5A744

The creators, Sam Chiet and Jesús A. Álvarez, did not provide hash functions. The hashes seen above were determined using VirusTotal.

### Discoveries

Desktop Goose can make computers lag very easily. Task Manager will show low CPU and Memory usage but the computer will stutter very heavily. This happens when another program needs more system resources. We also discovered that this program makes for the perfect trojan. Desktop Goose allows users to insert images, files, and code into the program's folder. From this feature, a malicious actor could easily insert arbitrary code that will allow them access to a victim's system. All under the guise of a harmless little goose.

### Challenges

We faced an issue running Desktop Goose using ANY.RUN. Desktop Goose is dependent on files that are extracted using DesktopGoose v0.3 Extractor. When uploading DesktopGoose v0.3

## Team 4 Final Report - Desktop Goose

Extractor.exe which provides all the files required for Desktop Goose to run, ANY.RUN creates a report for DesktopGoose v0.3 Extractor.exe instead of GooseDesktop.exe (Desktop Goose).

Therefore, we were unable to automatically generate indicators of compromise or the MITRE ATT&CK™ MATRIX.

## Static Analysis

### Virus Total

Virus Total generated the following information about Desktop Goose.

- Detection: 4/69
- Size: 226304 byte
- Creation Time: 2020-02-11 20:16:54 UTC
- First Seen In The Wild: 2020-02-11 12:16:54 UTC
- First Submission: 2020-02-11 20:46:24 UTC

Within the portable executable resource parents associated with the DesktopGoose.exe file is a Games.exe file that has 59/70 detections as being malicious. Although it is only listed as being moderately malicious, it is a file system that is commonly used as a source for malicious actors to inject trojans onto a target system.

Virus Total detected that DesktopGoose.exe has a Target Machine that uses Intel 386 or later processors and compatible processors. DesktopGoose also has an entry point of 206650 and contains 3 sections.

### Cuckoo Sandbox

Cuckoo Sandbox's static analysis gave Desktop Goose a score of 0.6/10 and labeled it benign. The portable execution (PE) compile timestamp for Desktop Goose was 2020-02-11 13:16:54.

# Team 4 Final Report - Desktop Goose

Static Analysis

[Strings](#)
[Antivirus](#)
[ISSUE](#)

PE Compile Time

2020-02-11 13:38:54

PDB Path

C:\Users\Start\_Ricecraft\Documents\Visual Studio 2013\Projects\GoozeDesktop\GoozeDesktop.vbproj\Release\GoozeDesktop.pdb

PE Imphash

F98D5F28577ed6f0ee553b155a344

Version Infos

Translation

0x0000 0x0400

LegalCopyright

Copyright 1x00 2020

Assembly Version

1.0.0.0

InternalName

GoozeDesktop.exe

FileVersion

1.0.0.0

CompanyName

LegalTrademarks

Comments

ProductName

GoozeDesktop

ProductVersion

1.0.0.0

FileDescription

GoozeDesktop

OriginalFilename

GoozeDesktop.exe

Sections

Name	Virtual Address	Virtual Size	Size of Raw Data	Entropy
.text	0x00002000	0x00030760	0x00030800	5.87024886186
.rsrc	0x00034800	0x00006664	0x00006800	7.82296961607
.rdata	0x0003ac00	0x0000000c	0x00000200	6.101934625663

Resources

Name	Offset	Size	Language	Sub-language	File type
RT_ICON	0x0003a100	0x00000018	LANG_NEUTRAL	SUBLANG_NEUTRAL	PNG image data, 256 x 256, 8 bit/color RGBA, non-interlaced
RT_GROUP_ICON	0x0003a104	0x00000014	LANG_NEUTRAL	SUBLANG_NEUTRAL	data
RT_VERSION	0x0003a128	0x0000003c	LANG_NEUTRAL	SUBLANG_NEUTRAL	data
RT_MANIFEST	0x0003a174	0x000001ee	LANG_NEUTRAL	SUBLANG_NEUTRAL	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators

Imports

Library names:dbi

0x652080 CorExeMain

Figure 1. Static Analysis page of Cuckoo Sandbox

### Interesting Section:

Name	Virtual Address	Virtual Size	Size of Raw Data	Entropy	MD5
.text	0x00002000	0x00030760	0x00030800	5.87024886186	49877307c9317b526165b24d02b5f69a
.rsrc	0x00034000	0x00006664	0x00006800	7.822961607	4337b64b22bcc4286ed8a39c0346225a
.reloc	0x0003c000	0x0000000c	0x00000200	0.101910425663	148dd848edf9ea2e74b914ab3ea246e2

Table 1. Information taken from Cuckoo Sandbox and VirusTotal.

## Imports

MSCOREE.DLL: Called when execution begins of a managed code Portable Executable (PE) file, which has a ".exe" suffix like a machine-language file but is different internally.



CorExeMain: Initializes the common language runtime (CLR), locates the managed entry point in the executable assembly's CLR header, and begins execution. From the mscoree.dll library.

## Strings

The following strings were taken from Ghidra.

- NabMouse
  - High possibility that NabMouse was called when the Goose takes the user's mouse when they close a window that the goose created.
- OpenPaypalLink
  - OpenPaypalLink was likely created to prompt the user for donations through PayPal.
- Make the goose try and steal your mouse!
  - Sam Chiet may have left comments within the code of Desktop Goose that was detected by Ghidra. Our team thought that was an interesting string.
- <https://i.redd.it/j2f1i6dx2p.31.jpg>
  - A link that opens an image of a goose that matches Meme5 from the Memes folder (Figure 2).

## Dynamic Analysis

### Program

Running the program creates a goose that wanders around the desktop, drags comedic images, and notepad text onto the screen. If you delete the pop-ups on the screen, the goose will begin to chase your cursor and take it from you, leaving you unable to use your mouse for a few seconds.

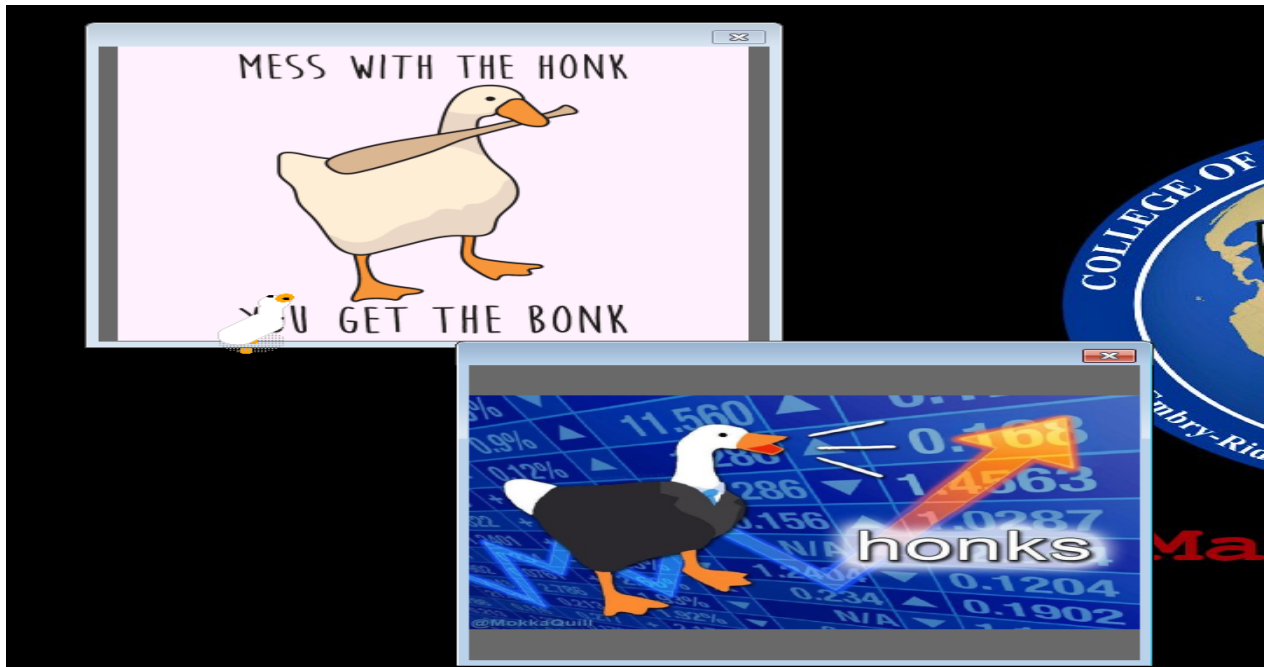


Figure 2: The goose walks around your screen and pulls pictures out.

### Resource Monitor

#### Processes with Network Activity

As seen in figure 4, Resource Manager detects no network Activity from DesktopGoose.exe.


Processes with Network Activity			
<input type="checkbox"/> Image	PID	Send (B/sec)	Receive (B/sec)
<input type="checkbox"/> svchost.exe (LocalServiceAndNoImpersonation)	1316	0	88
			

Figure 3. Processes with Network Activity detected by Resource Manager.

## CPU

Resource Manager uses approximately 24.42% of the CPU. This may hinder some activities that require a lot of CPU usage.

CPU <span>53% CPU Usage</span> <span>100% Maximum Frequency</span>						
<input type="checkbox"/> Image	PID	Descrip...	Status	Threads	CPU	Average CPU
<input type="checkbox"/> GooseDesktop.exe	772	Goose...	Running	48	18	24.42

Figure 4. Resource Manager.

## Process Tree

Cuckoo Sandbox's process tree showed that GooseDesktop.exe was the only running file that was detected when running the program. This may be because Cuckoo Sandbox does not allow for the upload of additional files.

### Behavioral Analysis

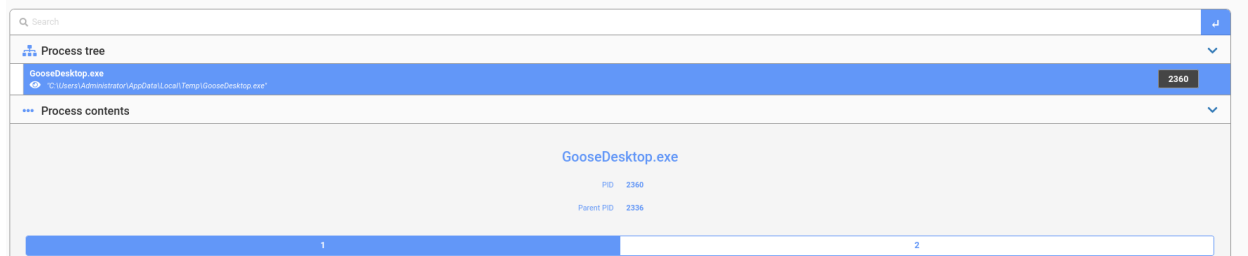


Figure 5. Behavior Analysis from Cuckoo Sandbox.

### Fakenet

Faknet confirms the finding of Resource Manager as it detected no network activity from DesktopGoose.exe.

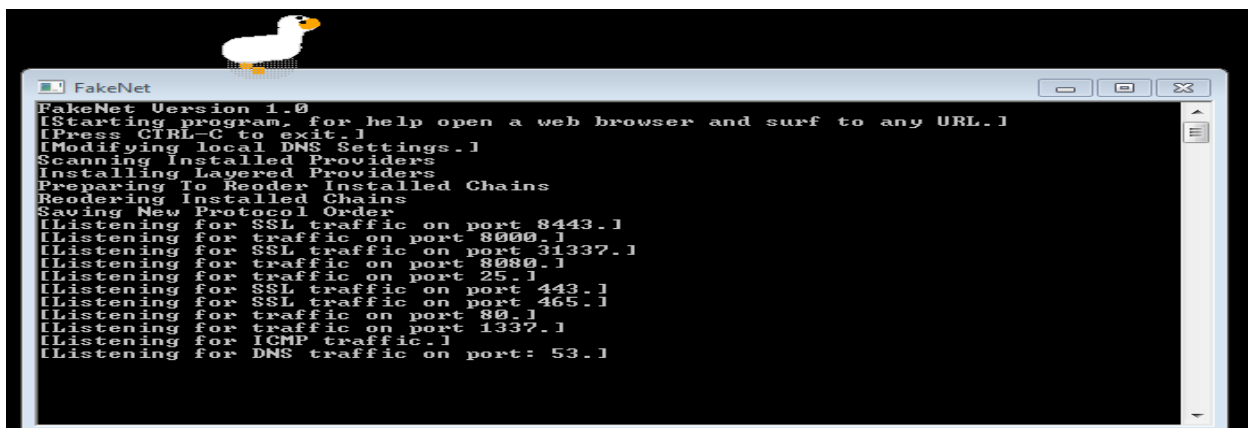


Figure 6. FakeNet results.

### Desktop Goose Dependent Files

The extractor creates several asset files for Desktop Goose. None of the files that Desktop Goose creates are encrypted and are shown in plain text as seen in Appendix 1. A point of interest may be the folder “Mods” seen in figure 13, as customization may be exploited to create a trojan.

ANY.RUN

In ANY.RUN DesktopGoose.exe was executed manually to allow for all file dependencies to be accessible. ANY.RUN gave DesktopGoose a 100 out of 100 for malicious intent. When running DesktopGoose ANY.RUN did not detect any modified files, registry changes, HTTP requests, connections, or network threats, however, there were 73 Modules detected as seen in figure 7. Danger was detected when DesktopGoose loaded then dropped or rewrote an executable and dropped or rewritten from another process. In both instances ANY.RUN notes that the processes were dropped.

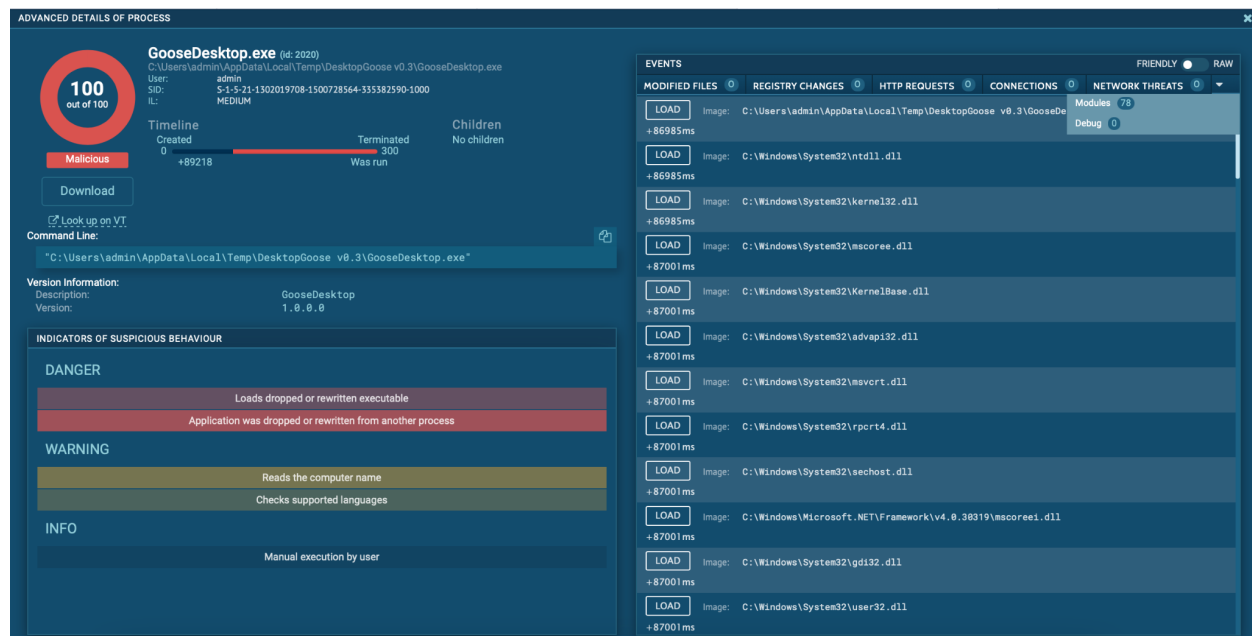


Figure 7. ANY.RUN analysis of GooseDesktop.exe

## Mitigations

There are multiple ways to mitigate the chances of infection from a malicious Desktop Goose. The first way to prevent infection is to not download the program or other random .exe files. This is the most effective way to keep malware off a system. Another way is to use an uninstaller such as Revo Uninstaller. This is an uninstaller for Windows systems. The main benefit of an uninstaller is that it deletes the registry entries that the uninstalled program may leave behind.

However, if a user wants to download Desktop Goose, ensure the download is from the official Samperson website and run an antivirus scan before the program is run. Also, if the program is downloaded and run as a prank, then it can be turned off by holding the escape button. The instructions in the programs folder make mention of this.

## Conclusion

Desktop Goose can be considered grayware malware. It is not inherently dangerous, but it can easily be turned into an avenue to send other malware. The fact that the program makes it easy to add in “mods”, may allow for trojan malware to infect the system. Despite this, it is relatively easy to mitigate being attacked by the goose. As stated earlier, not downloading .exe files from the internet is the only sure way to protect yourself against this. The second best, is to use the official site and run a scan on the program before running it.

## Bibliography

- ANY.RUN. (n.d.). *DesktopGoose v0.3 Extractor.exe (MD5: 4794142776C35938D65AEC9AAC022C2F) - Interactive analysis - ANY.RUN*. Retrieved April 15, 2022, from <https://app.any.run/tasks/7a67aa82-28a4-423a-9a02-686a9011e3c6/>
- Chiet, S. (n.d.). *Desktop Goose by samperson*. Desktop Goose. Retrieved April 15, 2022, from <https://samperson.itch.io/desktop-goose>
- Edgar, T., & Manz, D. (2017). *Research Methods for Cyber Security*. Elsevier Gezondheidszorg. <https://www.sciencedirect.com/science/article/pii/B9780128053492000029>
- J. (2021, September 15). *\_CorExeMain Function - .NET Framework*. Microsoft Docs. Retrieved April 15, 2022, from <https://docs.microsoft.com/en-us/dotnet/framework/unmanaged-api/hosting/corexemain-function>
- Milliner, J. (2021, July 20). *Desktop Goose*. Softonic. Retrieved April 15, 2022, from <https://desktop-goose.en.softonic.com/mac>
- Norton. (2015, August 31). *What is Grayware?* Norton UK Blog. Retrieved April 15, 2022, from [https://uk.norton.com/norton-blog/2015/08/what\\_is\\_grayware.html](https://uk.norton.com/norton-blog/2015/08/what_is_grayware.html)
- VirusTotal. (n.d.). *Virus Total*. Retrieved April 15, 2022, from <https://www.virustotal.com/gui/file/943fd1ea44266c5d7fa02f2b292db095a4e6ba8027a1f6c73fd60d1165e63aff/detection>

## Appendix 1 - Associated Files

DesktopGoose v0.3

Share View

> This PC > Downloads > DesktopGoose v0.3

Name	Date modified	Type	Size
Assets	2/8/2020 2:59 PM	File folder	
FOR MOD-MAKERS	2/9/2020 7:43 PM	File folder	
changelog	2/9/2020 7:37 PM	Text Document	3 KB
Close Goose	2/7/2020 1:22 PM	Windows Batch File	1 KB
config	2/9/2020 7:48 PM	Configuration sett...	1 KB
GooseDesktop	2/11/2020 1:16 PM	Application	221 KB
GooseModdingAPI.dll	2/9/2020 12:44 AM	Application exten...	16 KB
MMQ.dll	2/8/2020 2:55 PM	Application exten...	11 KB
patrons	2/9/2020 5:00 PM	Text Document	1 KB
Read me! Honk	2/9/2020 7:47 PM	Text Document	3 KB

Figure 8. Base directory of Desktop Goose

```

changelog.txt - Notepad
File Edit Format View Help
NEW IN VERSION 0.3
- CUSTOM NOT-EPAD TEXT ! Add whatever notepad phrases you want as text files in the "Assets/Text/NotepadMessages" folder, and the goose will pull them up!
- NEW MODDING API! Drop mods into their own folders in Assets/Mods/YourModNameHere, and toggle "EnableMods" in the config.ini! Build your own mods with the solution in the "F
- NEW CONFIG TOGGLES! Customize the goose's behaviour further, silence the audio, and more!

Bugfixes:
- Goose auto-releases mouse when it quits while stealing your cursor. No more having to alt-tab!
- Lifted multi-hundred meme 'soft-cap'. Now you crazy monsters can load even more memes at once. Crazy kids.

COMING SOON in v0.4+...
- Twitch Chat/Donations Integration (let the chat control the goose! donation messages!) when you own the soon-to-release "Desktop Goose for Twitch", or whatever it'll be cal
- Modding API updates!
- Native multi-goose support!

0.21 Hotfix
- Fixed the infamous "Red X" crash!

NEW IN VERSION 0.2
- UNLIMITED MEMES! Add whatever images you want to the memes folder, and the goose will pull them up!
- GIF SUPPORT! Add GIFs to the meme folder and Goose will bring you your infinite video
- HACK THE GOOSE! Adjust his aggression and a few other parameters, by opening config.goos in Notepad! More customization to come...

Bugfixes:
- Temp fix: No more crashing, on an edge-case donation image load failure, if you move the files around for some reason? (In general, don't move and delete files while the pr

COMING SOON in v0.3+...:
- Customize the goose note messages!
- Play a custom jukebox playlist!
- Better mod support? Join the discord at https://discord.gg/2d6WcNg and check the #goose-mods channel to see how this develops.

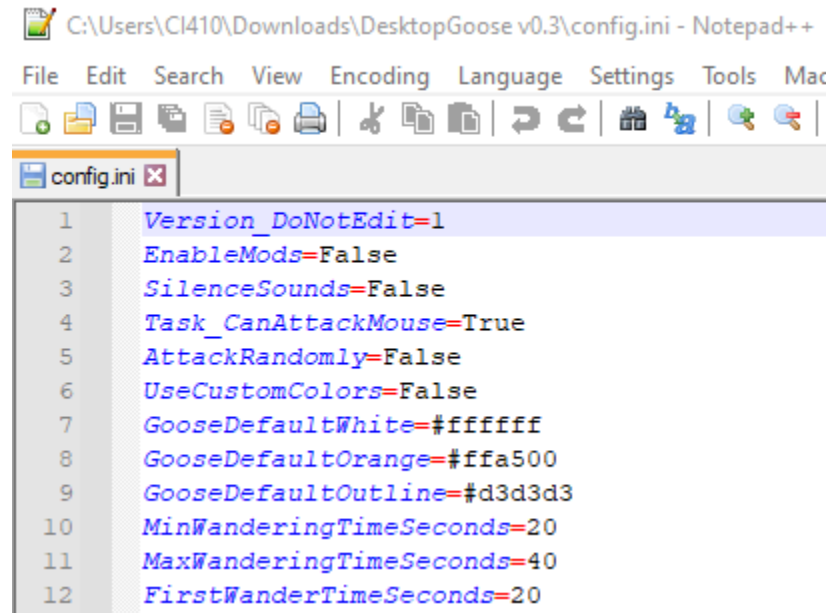
VERSION 0.1
This is just the base! We're only getting started

```

Ln 1, Col 1 90% Windows (CRLF) UTF-8

Figure 9. "changelog.txt" which follows the development of Desktop Goose.





```
1 Version_DoNotEdit=1
2 EnableMods=False
3 SilenceSounds=False
4 Task_CanAttackMouse=True
5 AttackRandomly=False
6 UseCustomColors=False
7 GooseDefaultWhite=#ffffff
8 GooseDefaultOrange=#ffa500
9 GooseDefaultOutline=#d3d3d3
10 MinWanderingTimeSeconds=20
11 MaxWanderingTimeSeconds=40
12 FirstWanderTimeSeconds=20
```

Figure 10. config.ini file which allows the user to tailor the Goose's actions to their liking.

## Team 4 Final Report - Desktop Goose



patrons.txt - Notepad

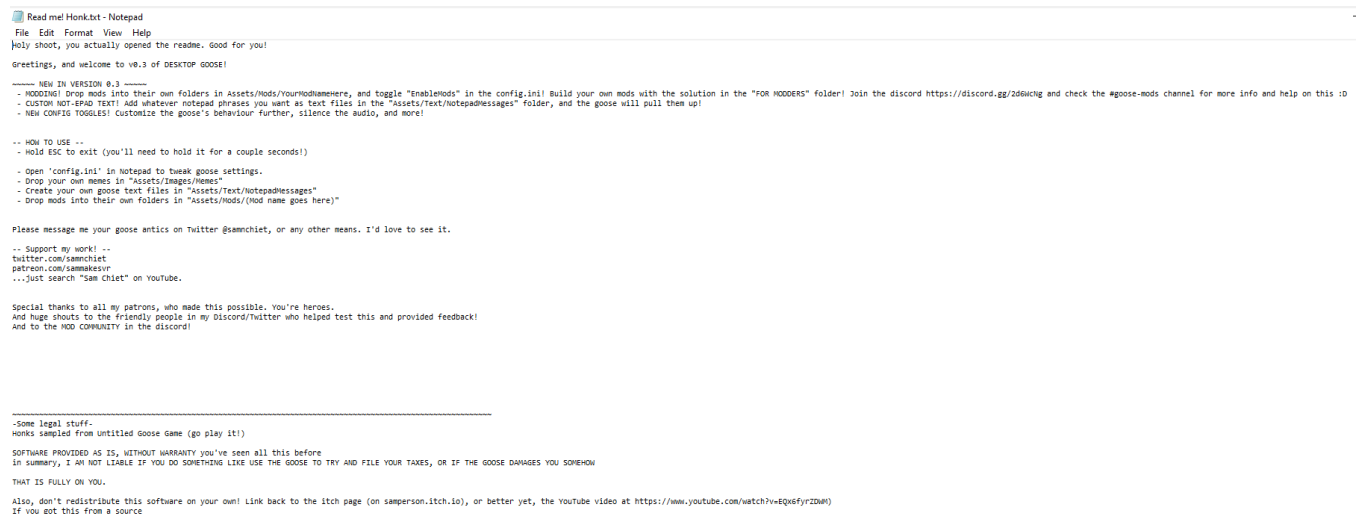
File Edit Format View Help

SPECIAL THANKS TO THE GLORIOUS PATRONS of patreon.com/sammakesvr (as of now on 2/10/2020)

=====

SideQuest  
-  
a sad lobster  
Ada Salazar  
Brysia Chan  
Mikeykiller77  
Mujin  
Pixel  
Shay  
Strollky  
TheBenefactor  
-  
Addison Wilson  
Andrew Davies  
baimgarbaim  
Billyds1324  
Bruce D Beagle  
Collin Palmer  
Commander Bork  
Demon\_Fire  
DFPRIDE  
dstayton  
Ghosty  
Goosejuce  
Jokesterr Zero  
Kanja  
Kevaid  
Kevin Pratama  
Kidjchai Yingsery  
Leah  
Lucas Rizzotto  
Maya Yellin  
mjtgreen  
moss\_  
Riley Davey  
Roland Fehér  
Rondell Paul  
Souhaib Haouache  
Tigwyk  
Tole Canal  
Vanessa Ramirez  
Vratislav Fidler

Figure 11. List of patrons that sponsored Sam Chiet as of February 10, 2020.



Read me! Honk.txt - Notepad

File Edit Format View Help

holly shoot, you actually opened the readme. good for you!

Greetings, and welcome to v0.3 of DESKTOP GOOSE!

----- NEW IN VERSION 0.3 -----

- MODDING! Drop mods into their own folders in Assets/Mods/YourModNameHere, and toggle "EnableMods" in the config.ini! Build your own mods with the solution in the "FOR MODDERS" folder! Join the discord <https://discord.gg/2d6w4tng> and check the #goose-mods channel for more info and help on this :D
- CUSTOM NOTEPAD TEXT! Add whatever notepad phrases you want as text files in the "Assets/Text/NotepadMessages" folder, and the goose will pull them up!
- NEW CONFIG TOGGLES! Customize the goose's behaviour further, silence the audio, and more!

-- HOW TO USE --

- HOLD ESC to exit (you'll need to hold it for a couple seconds!)
- Open 'config.ini' in Notepad to tweak goose settings.
- Drop your own memes in "Assets/Images/Memes"
- Create your own goose text files in "Assets/Text/NotepadMessages"
- Drop mods into their own folders in "Assets/Mods/(Mod name goes here)"

Please message me your goose antics on Twitter @samchiet, or any other means. I'd love to see it.

-- Support my work! --

twitter.com/samchiet  
patreon.com/sammakesvr  
...just search "Sam Chiet" on YouTube.

Special thanks to all my patrons, who made this possible. You're heroes.  
And huge shouts to the friendly people in my Discord/Twitter who helped test this and provided feedback!  
And to the MOD COMMUNITY in the discord!

-----

-Some legal stuff-  
Honks sampled from untitled goose game (go play it!)

SOFTWARE PROVIDED AS IS, WITHOUT WARRANTY you've seen all this before  
In summary, I AM NOT LIABLE IF YOU DO SOMETHING LIKE USE THE GOOSE TO TRY AND FILE YOUR TAXES, OR IF THE GOOSE DAMAGES YOU SOMEHOW  
THAT IS FULLY ON YOU.

Also, don't redistribute this software on your own! Link back to the itch page (on samperson.itch.io), or better yet, the YouTube video at <https://www.youtube.com/watch?v=Eq6fyr2DNP0>  
If you got this from a source

Figure 12. Read me! Honk lists what was updated, how to Use Desktop Goose, asks for support, and provides legal information.

## Team 4 Final Report - Desktop Goose

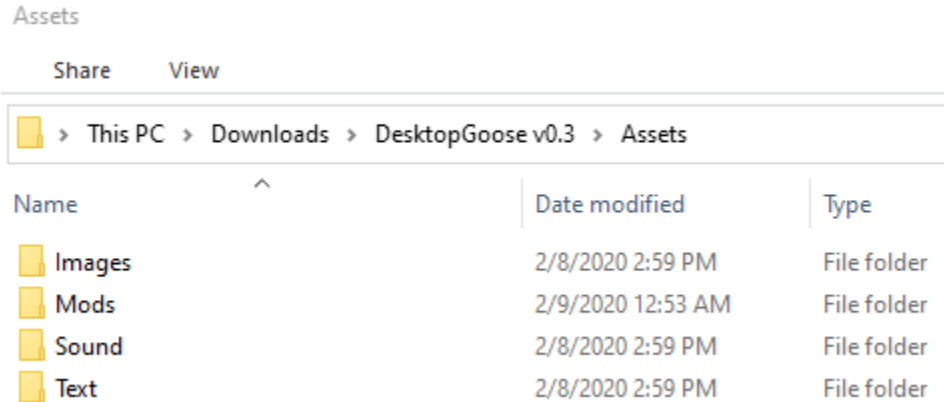


Figure 13. Assets of Desktop Goose

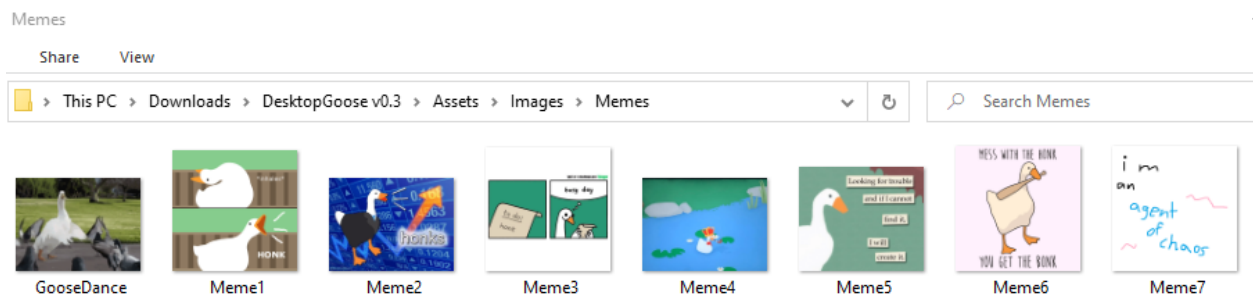


Figure 14. Image assets of Desktop Goose

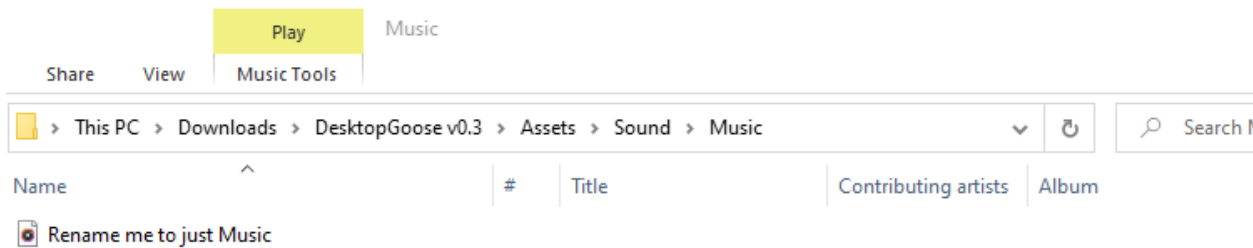


Figure 15. Music assets of Desktop Goose

## Team 4 Final Report - Desktop Goose

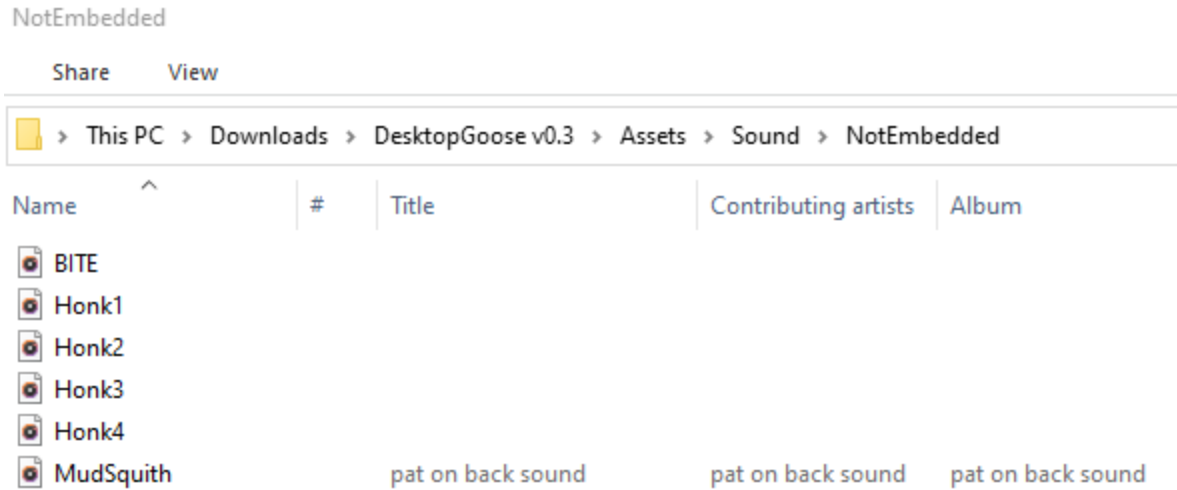


Figure 16. Not Embedded sounds from Desktop Goose

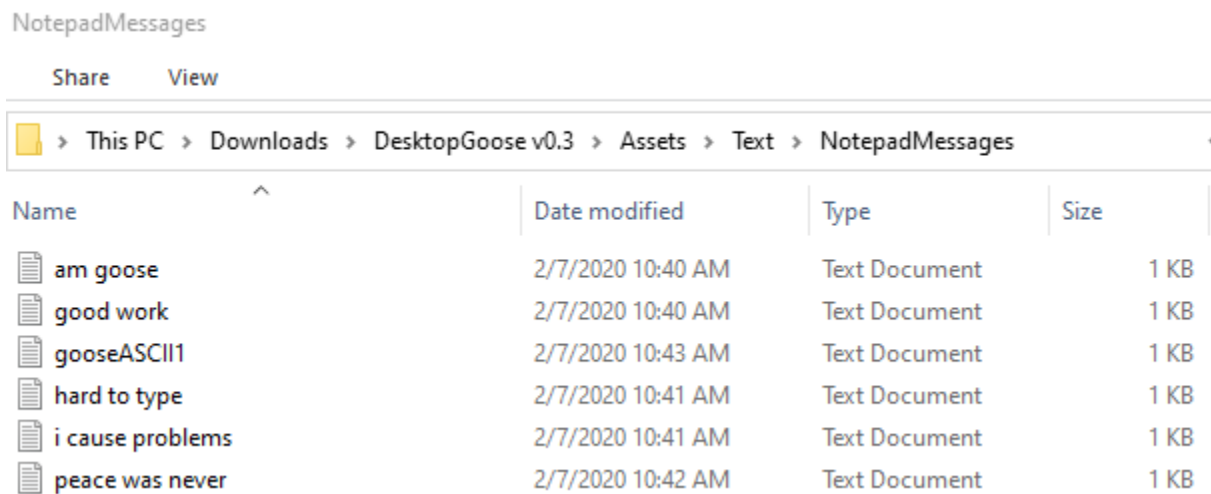


Figure 17. Notepad Messages from Desktop Goose

## Team 4 Final Report - Desktop Goose

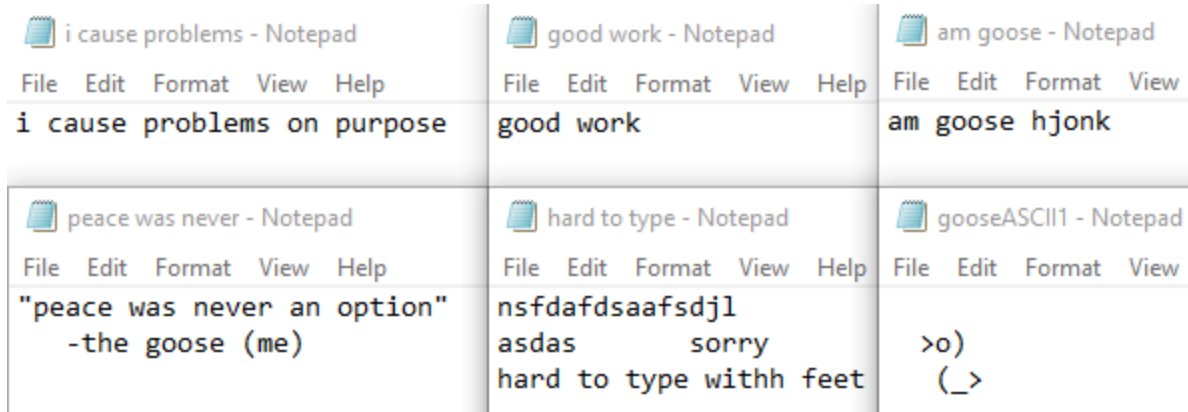


Figure 18. Messages within notepad created by Desktop Goose