GoaTracer

An open service for advanced PE analysis

Loria
Laboratoire lorrain de recherche en informatique et ses applications

cnrs

UNIVERSITÉ DE LORRAINE

Romain GUITTIENNE
Quentin JACQMIN
Jean-Yves MARION
Pierre MARTY
Fabrice SABATIER

GoaTracer

- **GoaTracer** is a free online sandbox for dynamically analyzing **PE files**
- You can use it via API or Web Interface
- It records every executed instruction and more
- It is hosted at the LHS, and is available for research purposes

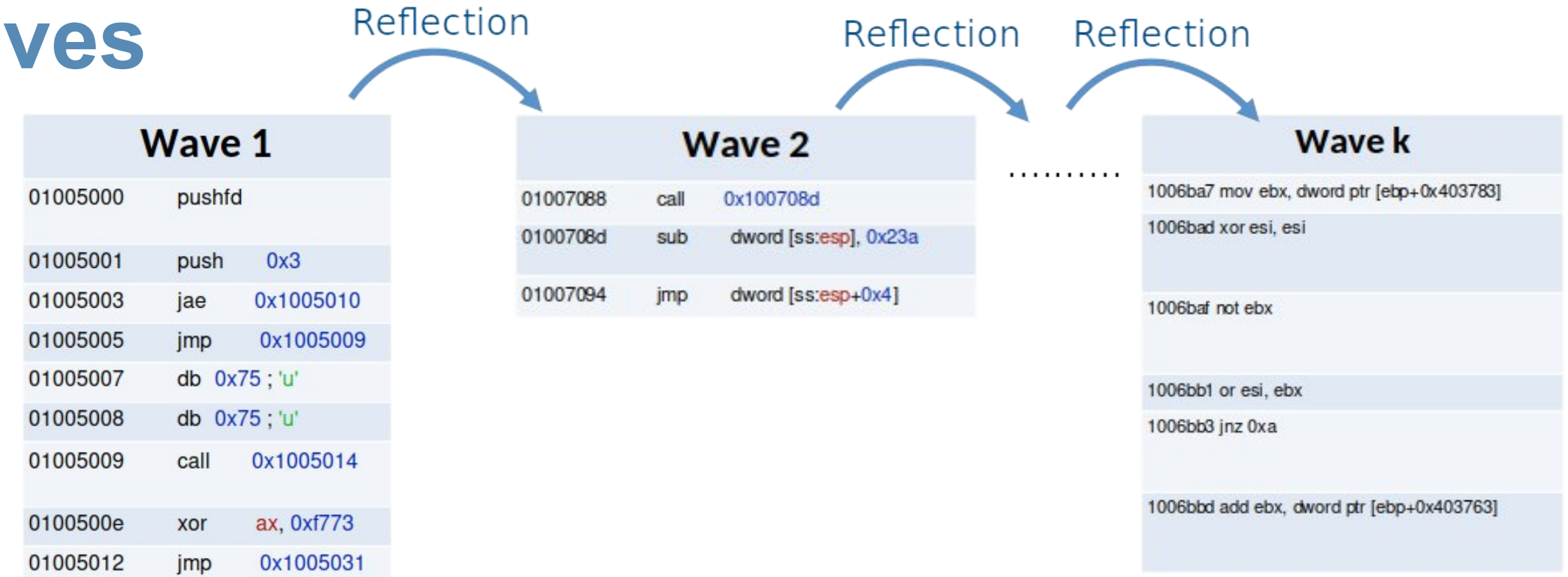
Loria
Laboratoire lorrain de recherche en informatique et ses applications

cnrs UNIVERSITÉ DE LORRAINE

Analysis tools

Free analysis tools	Full asm	Syscalls	Exceptions	Waves	CFG	CG	TTPs
GoaTracer 	✓	✓	✓	✓	✓	✓	✓
Drakvuf	✗	✓	✓	✗	✗	✗	✓
Any.run	✗	✓	✓	✗	✗	✗	✓
JoeSandbox	✓	✓	✓	✗	✗	✗	✓
Hybrid-analysis	✗	✓	✗	✗	✗	✗	✓
VMRay	✗	✓	✓	✗	✗	✗	✓
VirusTotal	✗	✓	✗	✗	✗	✗	✓
Homemade Pintool	✓	✓	✓	✓	✓	✓	✗

Waves



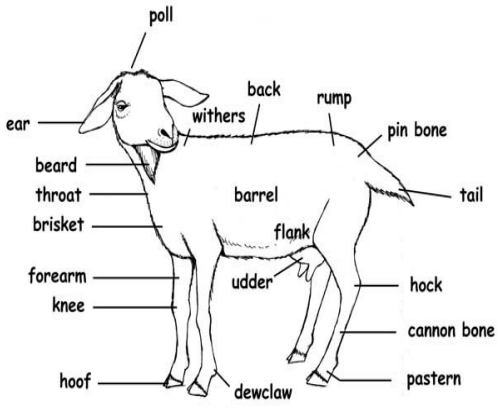
Represents self-modification, seen in unpacking layers

Loria
Laboratoire lorrain de recherche en informatique et ses applications

cnrs UNIVERSITÉ DE LORRAINE

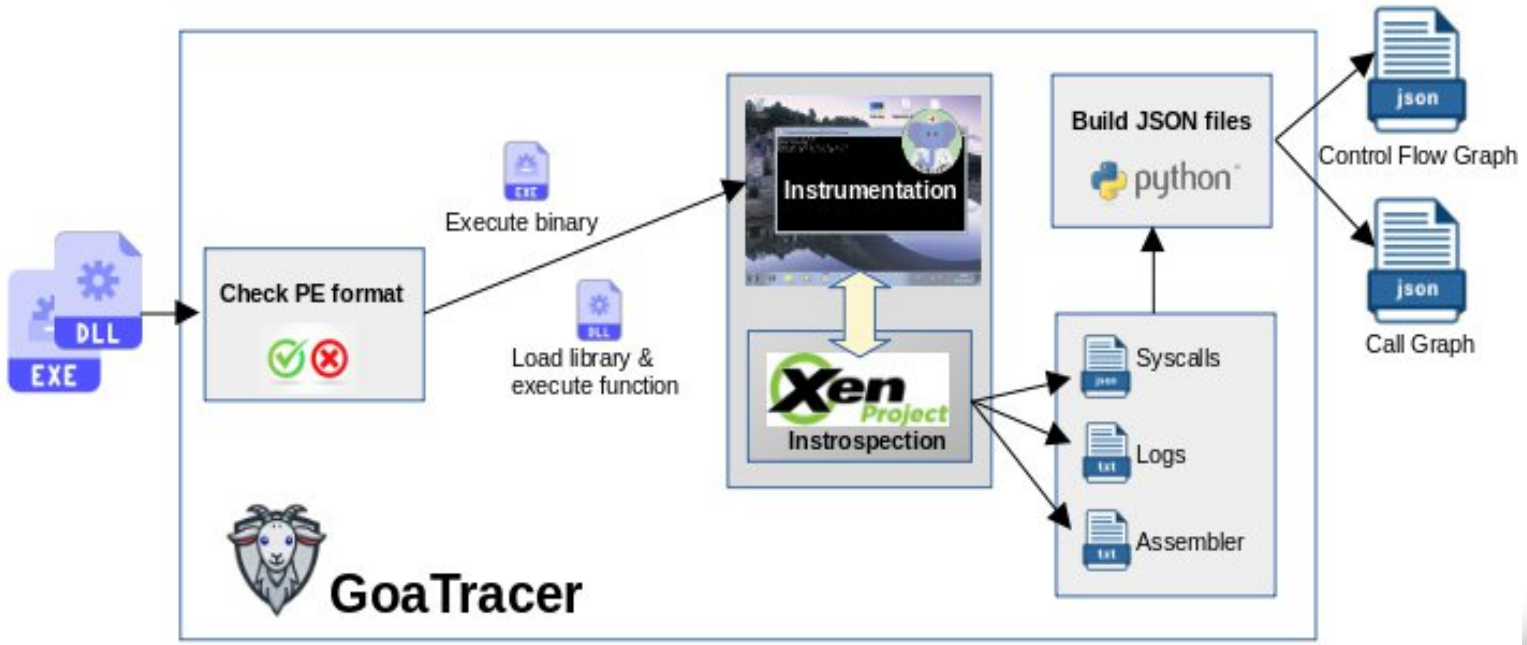
DEMO

Anatomy of the Goat



Uses two main technologies :

- DynamoRIO – Dynamic instrumentation
- LibVMI – Virtual machine introspection

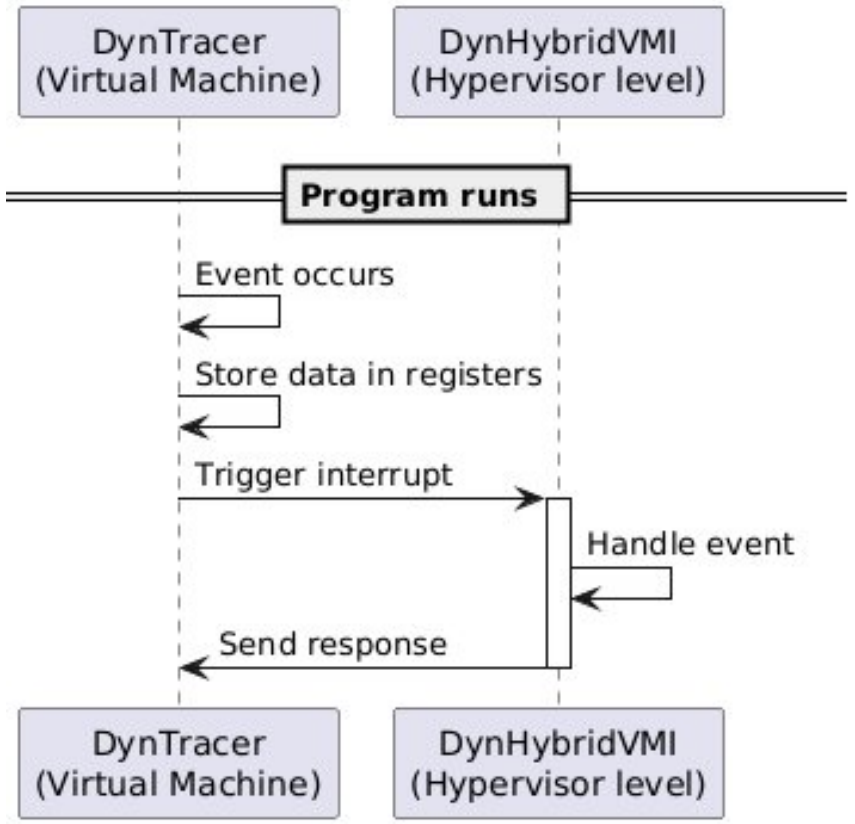


Loria
Laboratoire lorrain de recherche en informatique et ses applications

cnrs UNIVERSITÉ DE LORRAINE

Anatomy of the Goat

Communication between DynTracer and DynHybridVMI :



Loria
Laboratoire lorrain de recherche en informatique et ses applications

cnrs UNIVERSITÉ DE LORRAINE

Anatomy of the Goat

	Instrumentation (DynamoRIO)	Introspection (libVMI)	GoaTracer
Placement	Inside the program	Outside the VM	Inside/Outside
Scope	Program-level analysis	System-level analysis	Program and system level analysis
Impact	Alongside the execution	Non-instrusive (external monitoring)	Alongside the execution
Pros	Fine-grained analysis at the instruction level	Stealthy and not easily detectable	Instruction level analysis. Reasonably stealthy and difficult to detect
Cons	Instrusive and easily detectable	Higher-grained analysis, cannot output all executed instructions	

Stealth

Resilient against most known detection techniques

Tested on **Al-khaser**

Undetected by **pafish**

```
Administrateur : Invite de commandes - DynamoRIO9\bin32\drrun.exe -c DynTracerHybrid\dyntra...

[-] Wine detection
[*] Using GetProcAddress(wine_get_unix_file_name) from kernel32.dll ... OK
[*] Reg key (HKCU\SOFTWARE\Wine) ... OK

[-] VirtualBox detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key (HKLM\HARDWARE\Description\System "SystemBiosVersion") ... OK
[*] Reg key (HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions) ... OK
[*] Reg key (HKLM\HARDWARE\Description\System "VideoBiosVersion") ... OK
[*] Reg key (HKLM\HARDWARE\ACPI\DSDT\VBOX__ ... OK
[*] Reg key (HKLM\HARDWARE\ACPI\FADT\VBOX__ ... OK
[*] Reg key (HKLM\HARDWARE\ACPI\RSDT\VBOX__ ... OK
[*] Reg key (HKLM\SYSTEM\ControlSet001\Services\VBox* ... OK
[*] Reg key (HKLM\HARDWARE\DESCRIPTION\System "SystemBiosDate" ... OK
[*] Driver files in C:\WINDOWS\system32\drivers\VBox* ... OK
[*] Additional system files ... OK
[*] Looking for a MAC address starting with 08:00:27 ... OK
[*] Looking for pseudo devices ... OK
[*] Looking for VBoxTray windows ... OK
[*] Looking for VBox network share ... OK
[*] Looking for VBox processes (vboxservice.exe, vboxtray.exe) ... OK
[*] Looking for VBox devices using WMI ... OK

[-] VMware detection
[*] Scsi port 0,1,2 ->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key (HKLM\SOFTWARE\VMware, Inc.\VMware Tools) ... OK
[*] Looking for C:\WINDOWS\system32\drivers\vmmouse.sys ... OK
[*] Looking for C:\WINDOWS\system32\drivers\vmhgfs.sys ... OK
[*] Looking for a MAC address starting with 00:05:69, 00:0C:29, 00:1C:14 or 00:5
0:56 ... OK
[*] Looking for pseudo devices ... OK
[*] Looking for VMware serial number ... OK

[-] Qemu detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key (HKLM\HARDWARE\Description\System "SystemBiosVersion") ... OK

[-] Cuckoo detection
[*] Looking in the TLS for the hooks information structure ... OK


[-] Feel free to RE me, check log file for more information._
```

Loria
Laboratoire lorrain de recherche en informatique et ses applications

cnrs UNIVERSITÉ DE LORRAINE

Usecase 1 : Packers

Packer name	Execution time	# Waves
acpacker	00h03m48s	159
themida18	00h03m25s	106
acprotect	00h12m01s	99
pespin	00h01m44s	91
telock	00h00m30s	16
yodaprotect	00h02m02s	5
jdpack	00h32m24s	3
mystic	00h00m32s	3
aspack	00h00m11s	2
fsg	00h00m14s	2

Packer name	Execution time	# Waves
mew	00h00m21s	2
boxedApp	00h42m21s	1
epprotect	00h00m04s	1
neolite	00h00m09s	1
npack	00h00m12s	1
packman	00h00m12s	1
rlpack	00h00m12s	1
upx	00h00m09s	1
expressor	00h00m13s	1
vmprotect	00h00m05s	0

Usecase 2 : Malware (Lockbit)

Lockbit 4.0 API hashing [1] :

1) Searches inside the .dll
2) Looks for the address of an API, but **stops a few bytes before**
3) XOR the result **to get the actual address**
4) Calls the API

More difficult to detect which API is called

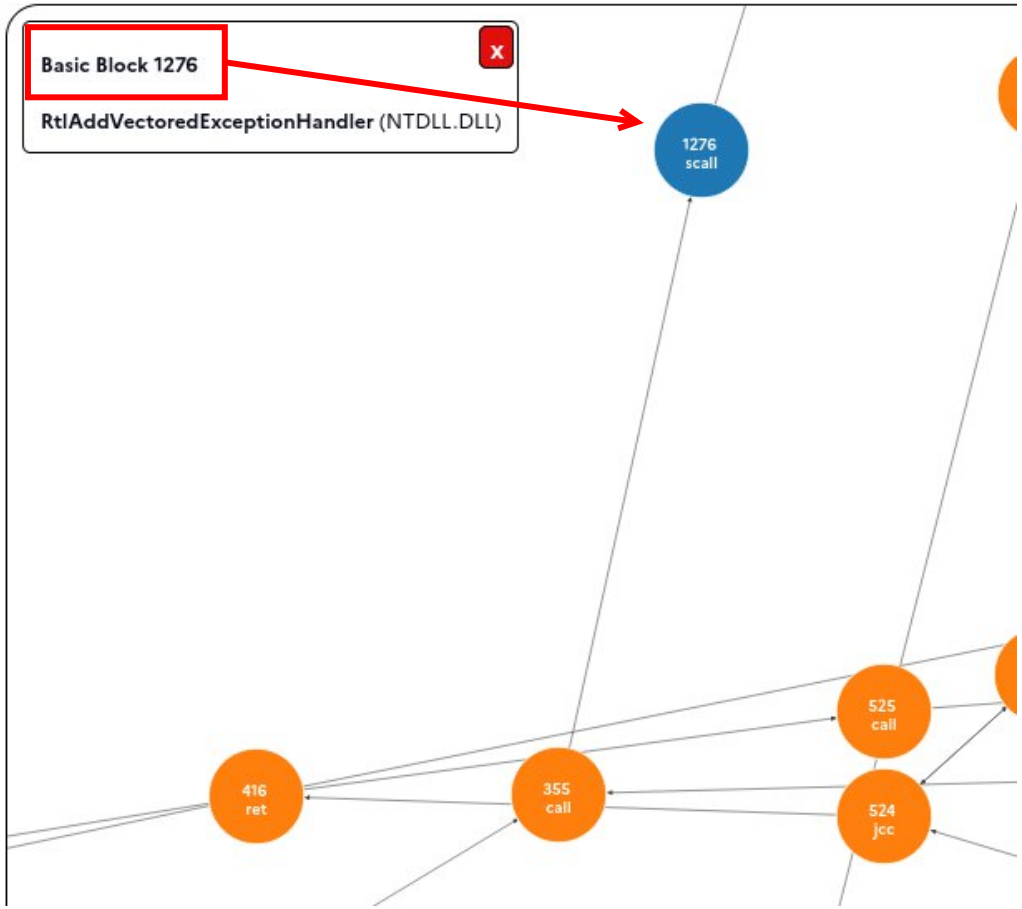
Loria
Laboratoire lorrain de recherche en informatique et ses applications

cnrs UNIVERSITÉ DE LORRAINE

Usecase 2 : Malware (Lockbit)

LOCKBIT 4.0

Let's take *RtlAddVectoredExceptionHandler* :



Windows API Functions calls

Timestamp	Name
52.867071	VirtualProtect
52.876537	VirtualProtect
216.899624	RtlAddVectoredExceptionHandler
217.422922	RtlRemoveVectoredExceptionHandler

Loria
Laboratoire lorrain de recherche en informatique et ses applications

cnrs UNIVERSITÉ DE LORRAINE

Usecase 2 : Malware (Lockbit)

LOCKBIT 4.0

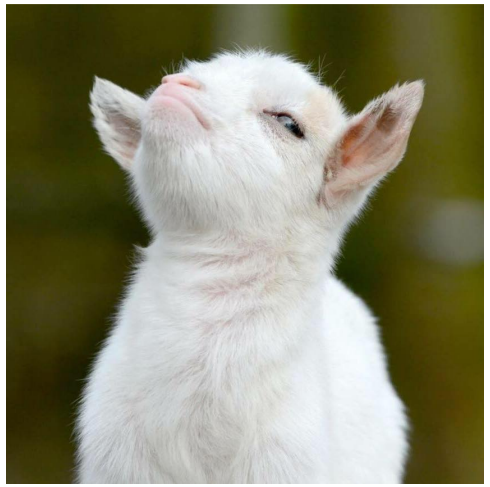
	GoaTracer	Drakvuf	Any.run [2]	JoeSandbox [3]	Hybrid-analysis [4]	VMRay [5]	VirusTotal [6]
Bypass obfuscation	✓	✗	✗	✗	✗	✓	✗

Loria
Laboratoire lorrain de recherche en informatique et ses applications

cnrs UNIVERSITÉ DE LORRAINE

Usecase 2 : Malware (Lockbit)

	GoaTracer	Drakvuf	Any.run [2]	JoeSandbox [3]	Hybrid-analysis [4]	VMRay [5]	VirusTotal [6]
Bypass obfuscation	✓	✗	✗	✗	✗	✓	✗



But remember that VMRay doesn't output the asm instructions for example !

Future works

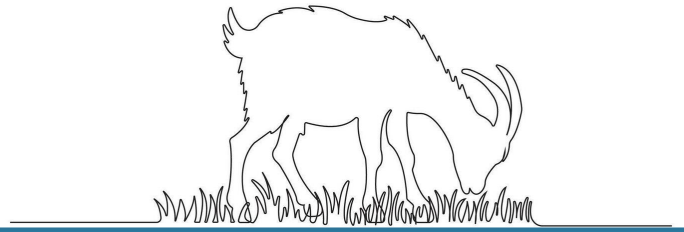
- Add Windows 10 VMs
- Extract payload from packed binaries
- Memory dump at each wave transition
- List obfuscations made by the PE file

Loria
Laboratoire lorrain de recherche en informatique et ses applications

cnrs UNIVERSITÉ DE LORRAINE

Key takeaways

- GoaTracer, a free online sandbox to analyze PE files
- Outputs asm instructions, syscalls, waves, CFG, CG, ...
- A combination of **precision** and **stealth**



How to access GoaTracer

Available at goatracer.lhs.loria.fr

You can request an account at loria-goatracer-contact@univ-lorraine.fr

Loria
Laboratoire lorrain de recherche en informatique et ses applications

cnrs UNIVERSITÉ DE LORRAINE

Thank you !

Loria
Laboratoire lorrain de recherche en informatique et ses applications

cnrs
UNIVERSITÉ DE LORRAINE

References

[1] https://elis531989.medium.com/green-with-evil-analyzing-the-new-lockbit-4-green-7f5783c4414c

[2] https://app.any.run/tasks/dc548c6f-2a6c-463b-b02a-4fd01adc1f21/

[3] https://www.joesandbox.com/analysis/1579250/0/html

[4] https://www.hybrid-analysis.com/sample/3552dda80bd6875c1ed1273ca7562c9ace3de2f757266dae70f60bf204089a4a/679a264151a027b688095dbc

References

[5] https://www.vmray.com/analyses/_mb/3552dda80bd6/report/behavior_grouped.html

[6] https://www.virustotal.com/gui/file/3552dda80bd6875c1ed1273ca7562c9ace3de2f757266dae70f60bf204089a4a/behavior

Loria
Laboratoire lorrain de recherche en informatique et ses applications

cnrs UNIVERSITÉ DE LORRAINE

Images sources

https://toppng.com/show_download/121199/goat-png

https://cyber-in-nancy.loria.fr/

https://en.wikipedia.org/wiki/Place_Stanislas#/media/File:Vue_de_nuit_de_la_Place_Stanislas_%C3%A0_Nancy.jpg

www.wildfilmsindia.com

https://www.exploringnature.org/db/view/Goat