Taurus Stealer's Evolution

blog.minerva-labs.com/taurus-stealers-evolution

- Tweet
-

Recently, we have seen a spike in events associated with Taurus stealer. The individual/s developing this threat have been actively improving the evasiveness of their loader since February 2021, which in turn made their payloads fully undetectable for almost a month.

Taurus AutoIt payload initial VirusTotal detection rates, taken from Nextron Systems' Valhalla:

(Nextron Systems)

The image depicts the latest Taurus payloads uploaded to VirusTotal and their initial positives rate, as can be seen in the table, no more than one vendor blacklisted these payloads, whereas most of these samples have been completely ignored by the industry's top anti-virus engines.

Some great technical blogs have already been published about this malware family by Zscaler, StrangerealIntel and TrendMicro, that is why the scope of the article is mainly the changes made since these publications. The goal of this technical analysis is to help the security community detect this threat and prevent it.

LOLbins & 7zip's SFX:

The initial infection begins with a zip file, masquerading as legitimate software, which contains a malicious SFX binary. The SFX binary drops several files to the user's temp directory:

- Dai.xlsm – a malicious AutoIt script.
- Puo.gif – an encrypted PE file.
- Scoute.dll - AutoIt binary, stripped of its MZ magic bytes.
- Dimagrato.accde – an obfuscated batch script.

Dimagrato.accde (batch script) is the next link in the chain, this small batch script was obfuscated to the size of 116 KB.

A snippet from Dimagrato.accde:

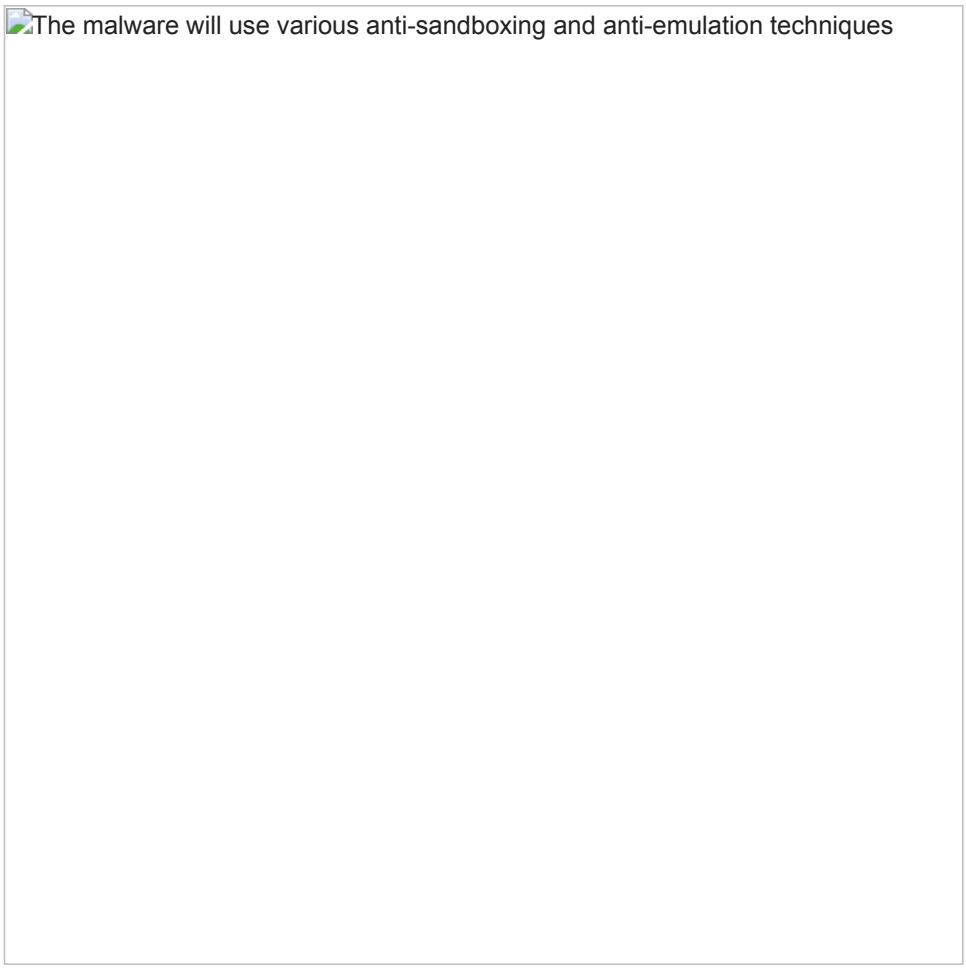
After de-obfuscation:

First, the script checks if the %userdomain% environment variable is equal to the string “DESKTOP-QO5QU33”, our guess is that this is an emulation detection technique. It then creates the AutoIt interpreter binary by replacing the prefix of Scoute.dll with the magic bytes MZ, and the now-valid binary is renamed to “Ali.com”. Finally, Ali.com is executed with Dai.xlsm as its command line parameter.

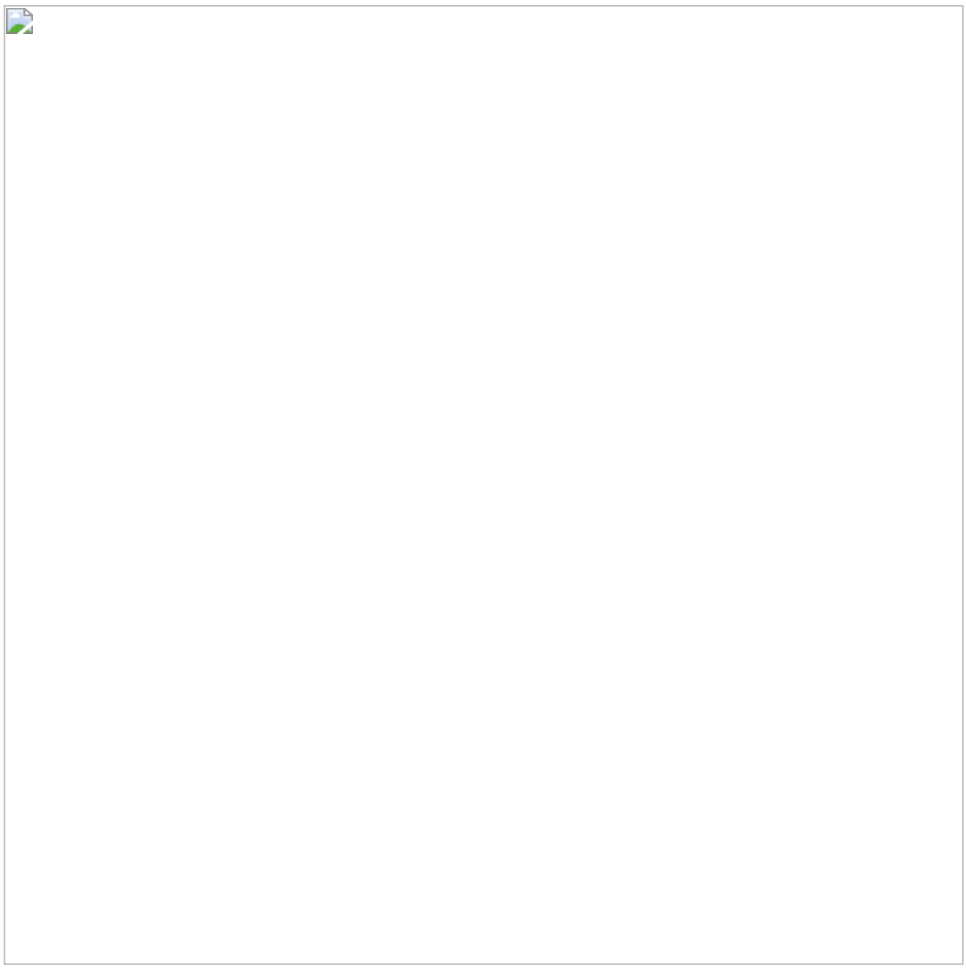
The AutoIt Script:

The main module of this attack is a highly obfuscated AutoIt script, it uses evasion techniques to avoid analysis and sandbox environments and then launches the actual stealer in-memory.

The malware will use various anti-sandboxing and anti-emulation techniques, beginning with computer name check and Microsoft Defender emulator file (aaa_TouchMeNot_.txt):

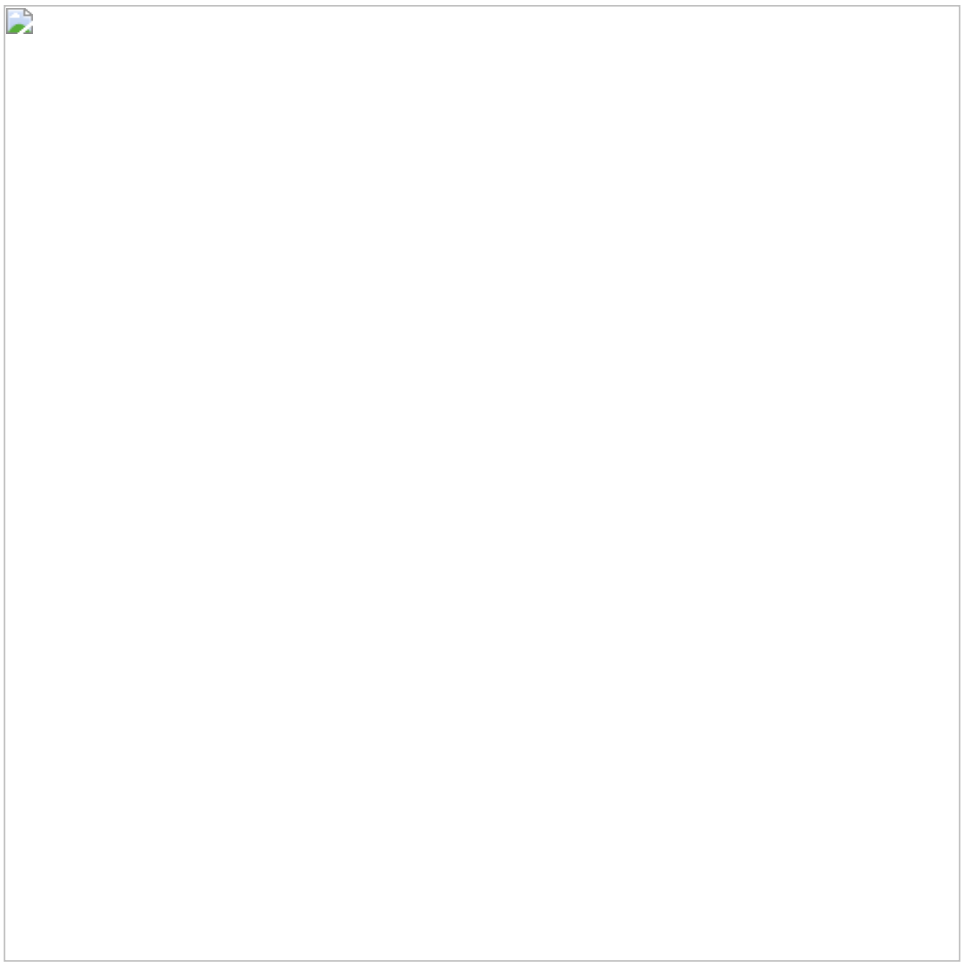


Another interesting anti-emulation trick used by the malware through the windows API SetErrorMode:



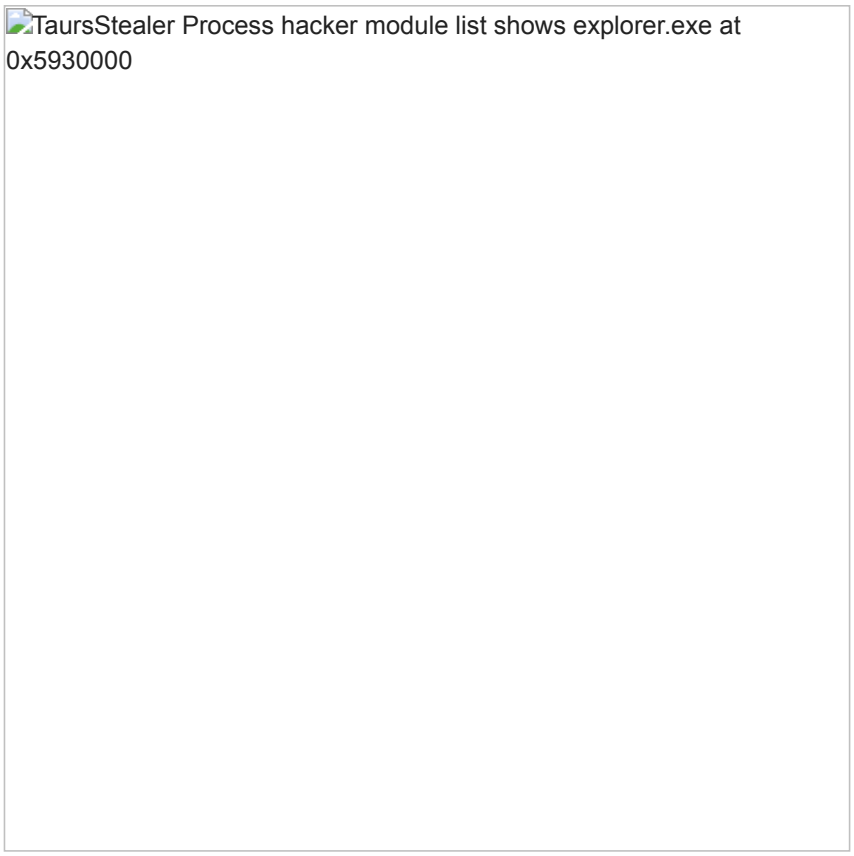
Taurus uses a computation based anti-analysis technique by calculating the sum of the Basel problem, deriving π from it (square root times six of the sum) and exiting if a number larger then π is the answer:

The last self-terminating evasion technique is a DNS killswitch. The malware will ping a specific domain and will exit upon successful connection:

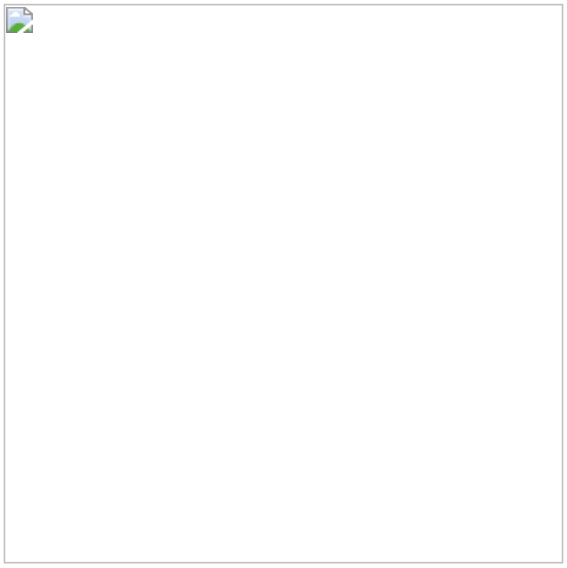


After being completely sure it is executing in a “safe” environment, the malware will read the file Puo.gif and decrypt it in-memory, the result is a PE file that will be reflectively loaded. Yet again the malware tries to fool security products, by loading the file explorer.exe into its memory space (using the LoadLibraryExW API) and overwriting the shared sections created by Windows OS with the decrypted malware. This technique may be used to fool security products that rely on the image linked to Windows section objects.

Process hacker module list shows explorer.exe at 0x5930000:



The actual allocation is a private RWX section:



Conclusion:

Over the past months Taurus has increased its evasiveness significantly, mutating each time it is covered by a security vendor. We expect this trend to continue with the release of the blog and encourage further security research of this threat, in favor of a robust prevention mechanism.

The infection process chain, as depicted by Minerva's platform:

IOCs:

Hashes:

61f3c3be1ae733d923f414205c0056a140fd9e279566bf6e83cf49931b445f67 (Dimagrato.accde)

a79b246d81ec3611228c4a545e02e83dd4196f8f4f470ca1f21470e87cfc76e8 (deobfuscated Dimagrato.accde)

5cfa9d6c4be74da3960e0973f29fc0aaf60b423be548fb5b409df648e3b49788 (Dai.xlsm)

46f2677e2c7a8d3207da130b8ab90233a5a28715593e717117690215e4fe6fc0 (decrypted PE Payload)

2002fc160b41b29863e8c7a85c932b052eea8651560f74b3b77a4514c5431d99 (Pou.gif)

Domains:

lisayt15[.]top

morlisanem01[.]top

disayta09[.]top/download.php?file=lv.exe

OsCvWtwAmcuANjreVoEpgBTcgNL[.]OsCvWtwAmcuANjreVoEpgBTcgNL