Preventing AgentTesla Infiltration

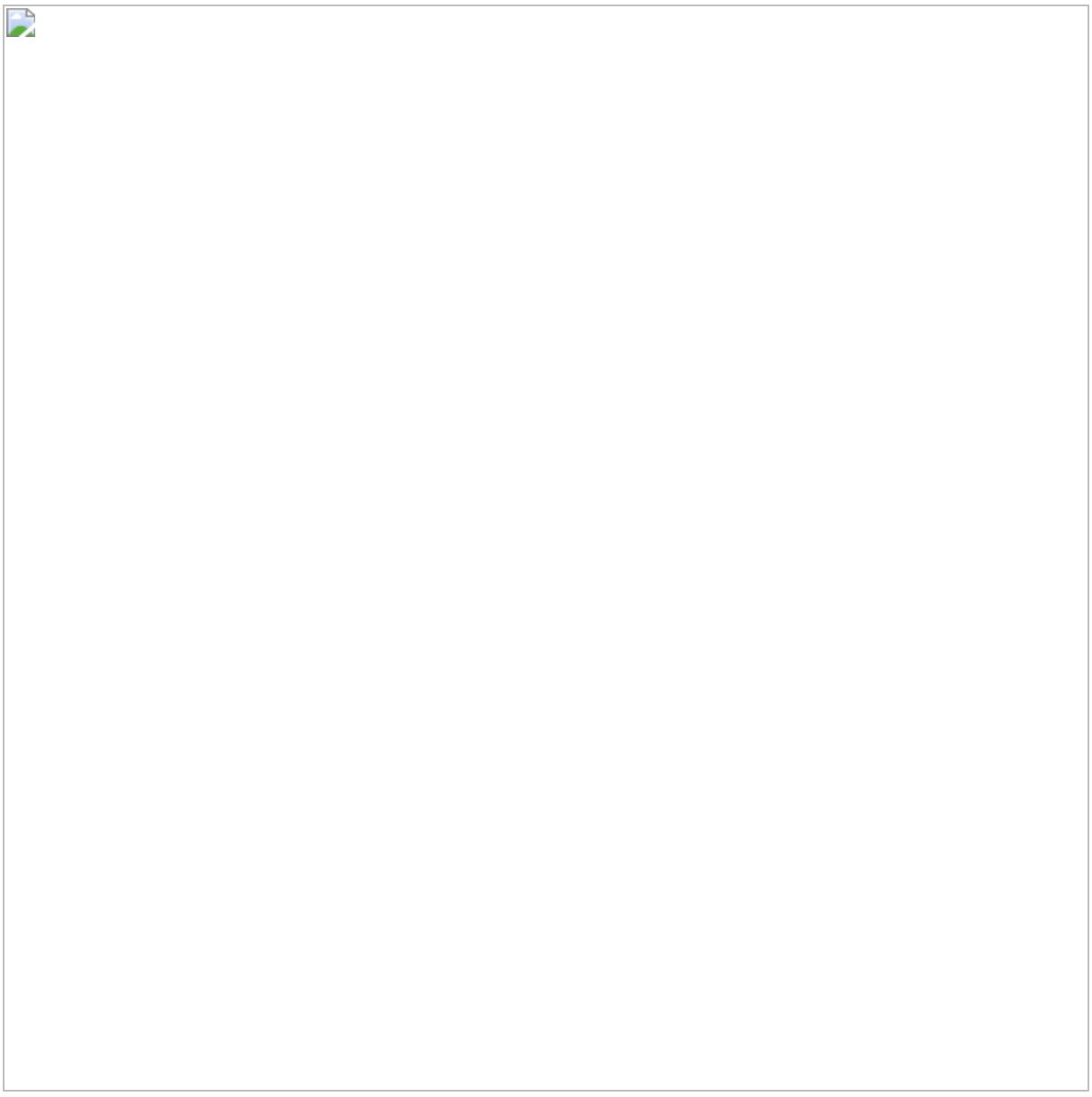
blog.minerva-labs.com/preventing-agenttesla

- Tweet
-

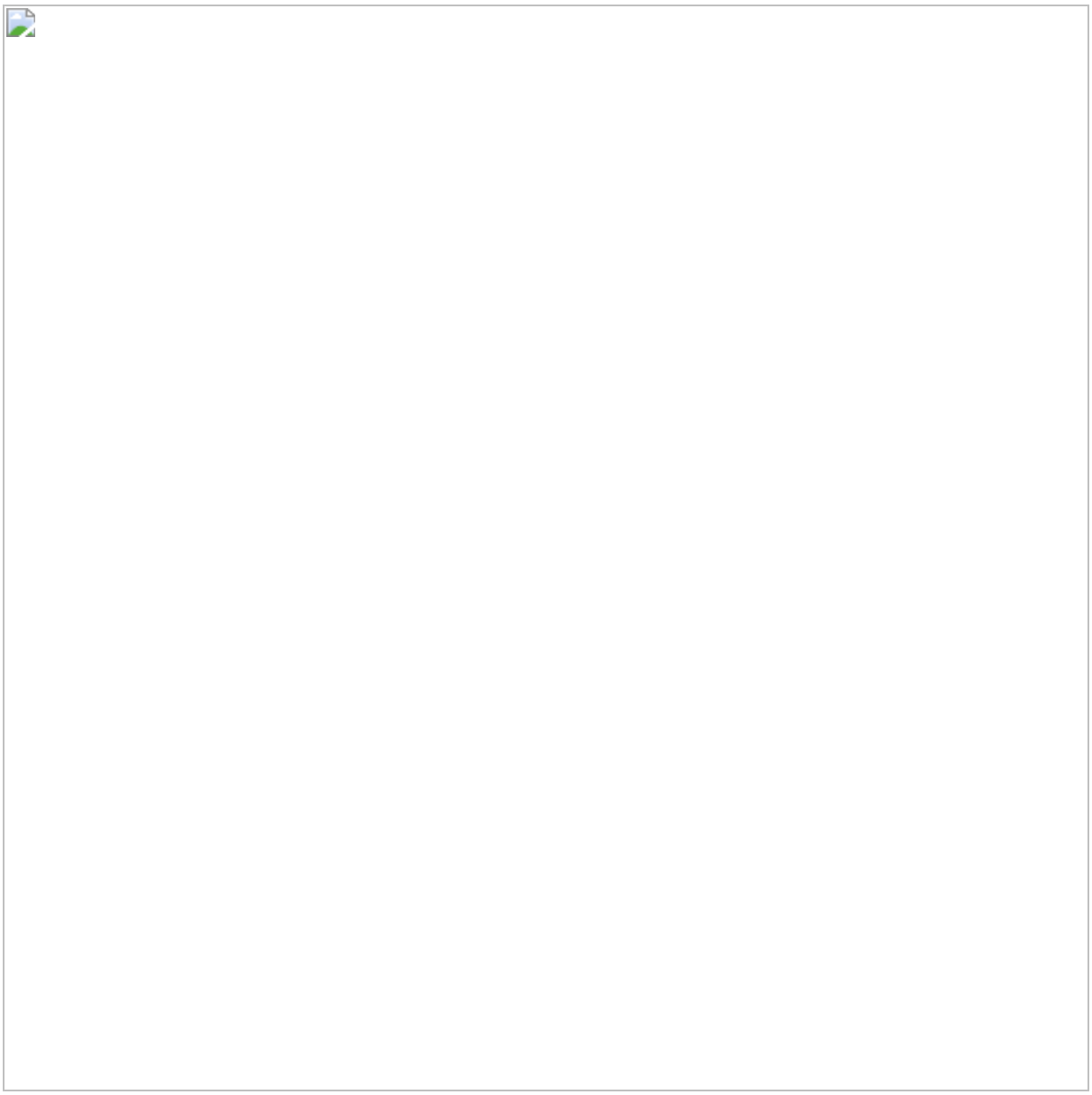
AgentTesla is a .NET based malware, commonly distributed as part of a malspam campaign. Use of AgentTesla soared in 2020, when it became a favorite of threat actors, which used it to achieve initial foothold on devices.

The sample we analyzed is a heavily obfuscated .NET binary, with a lot of redundant code that is there to confuse analysts. The actual decryption of the second stage is done when activating the set function of the attribute Form1.name, which will decrypt the next payload, load it and invoke it.

The payload decryption routine:

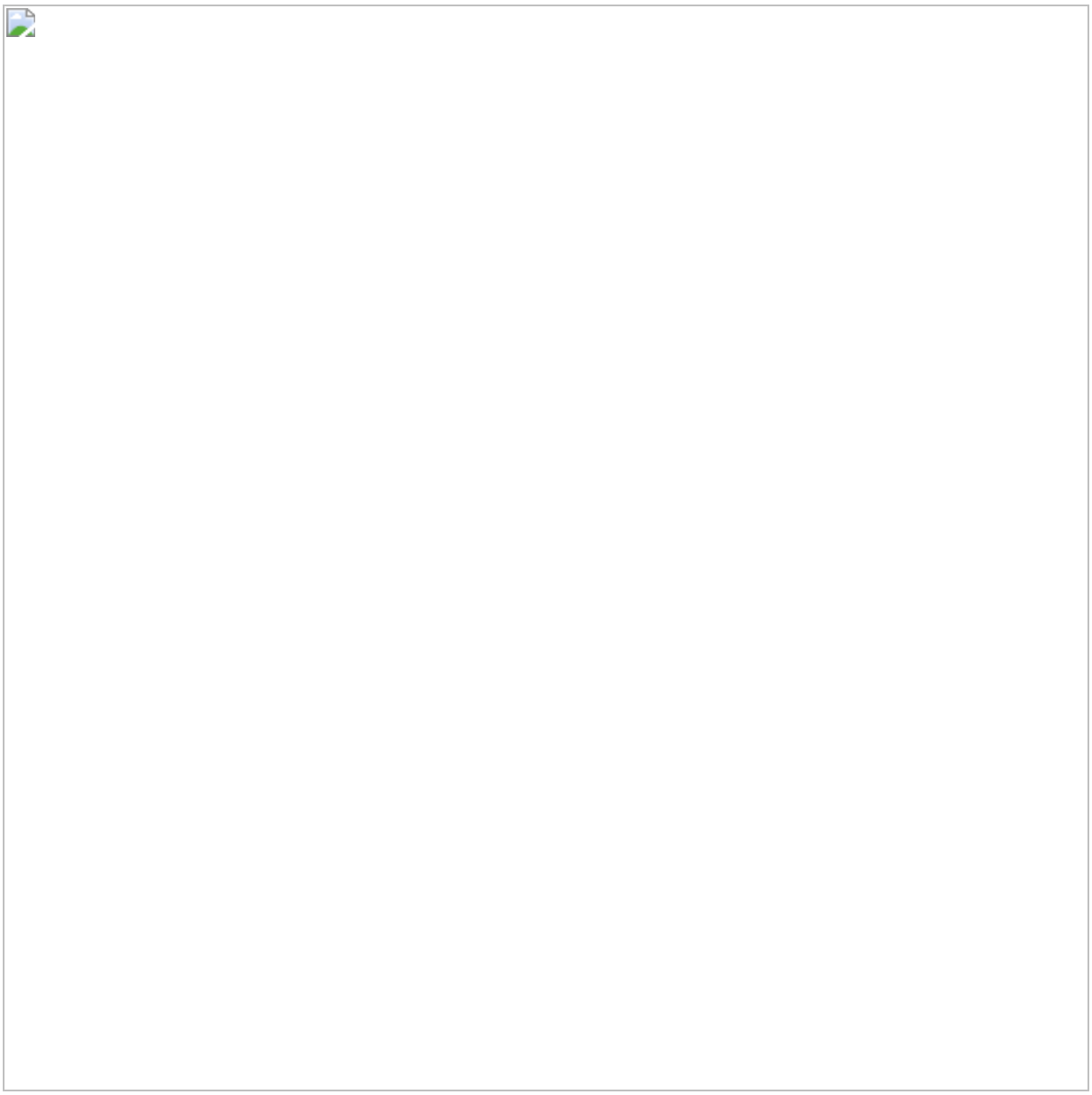


In memory loading in the property set routine:



The malware checks if it is executing in a sandboxed environment by querying for the loaded module “sbiedll.dll”, which is Sandboxie’s DLL. It will not execute if it is found. Minerva Prevents this AgentTesla variant with our Hostile Environment simulation module, using the malware’s code against it.

The event as depicted by Minerva’s platform:



IOCs:

Hashes:

405694b8ab3ca1034423bba6c91dc83831780e9de311b761fcd5d18e84093781

DNS:

smtp[.]yatchbabara[.]com

« Previous Post
Next Post »

Interested in Minerva? Request a Demo Below