RAT.Uknown.Malware2

RAT.Uknown.Malware2

Hashes

md5==>

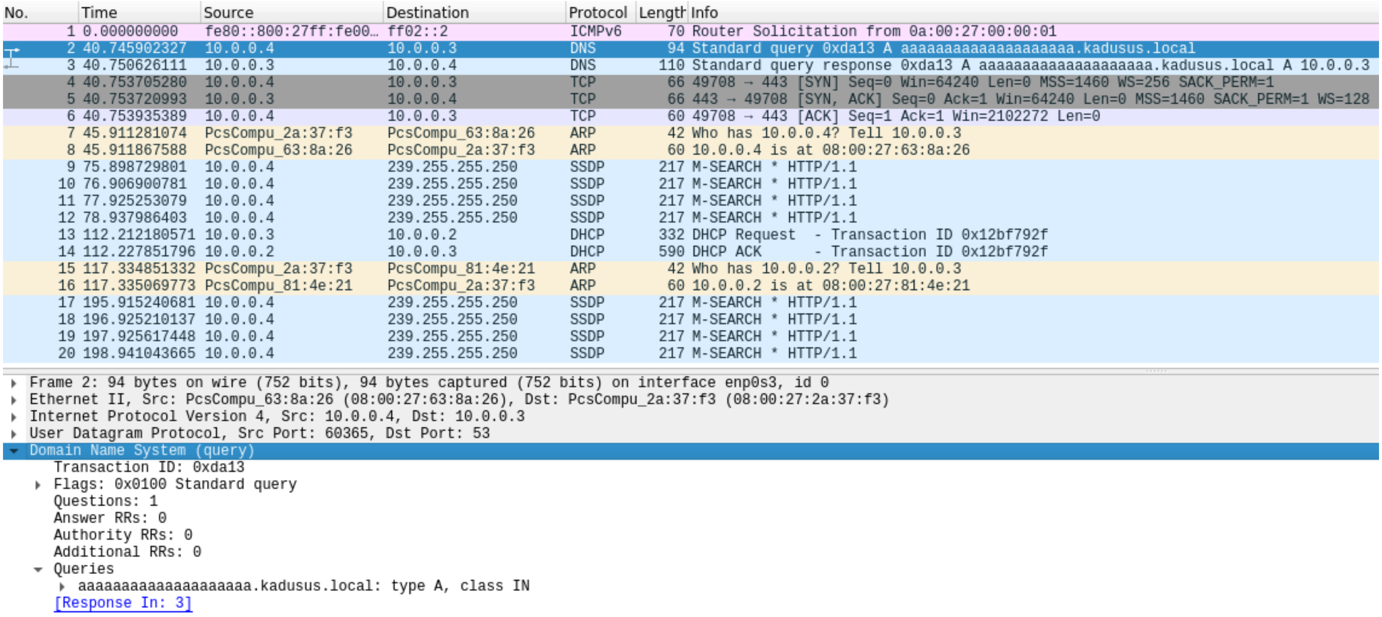
c211704777e168a5151de79dc87ffac7 RAT.Unknown2.exe.malz

SHA256==>

c522e0f1f9edb7e03c0a770e4c52a93db72dce21e7247322f4bbd5b053b967aab5240ce90d6aa65a79e3a3068f227346bf0190f9ca762fb8e8d076a58490d7a1 RAT.Unknown2.exe.malz

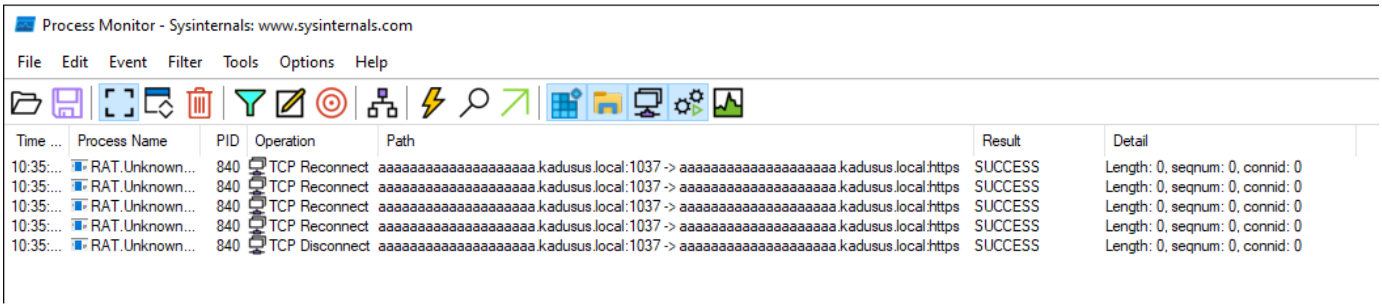
---

Dynamic Analysis

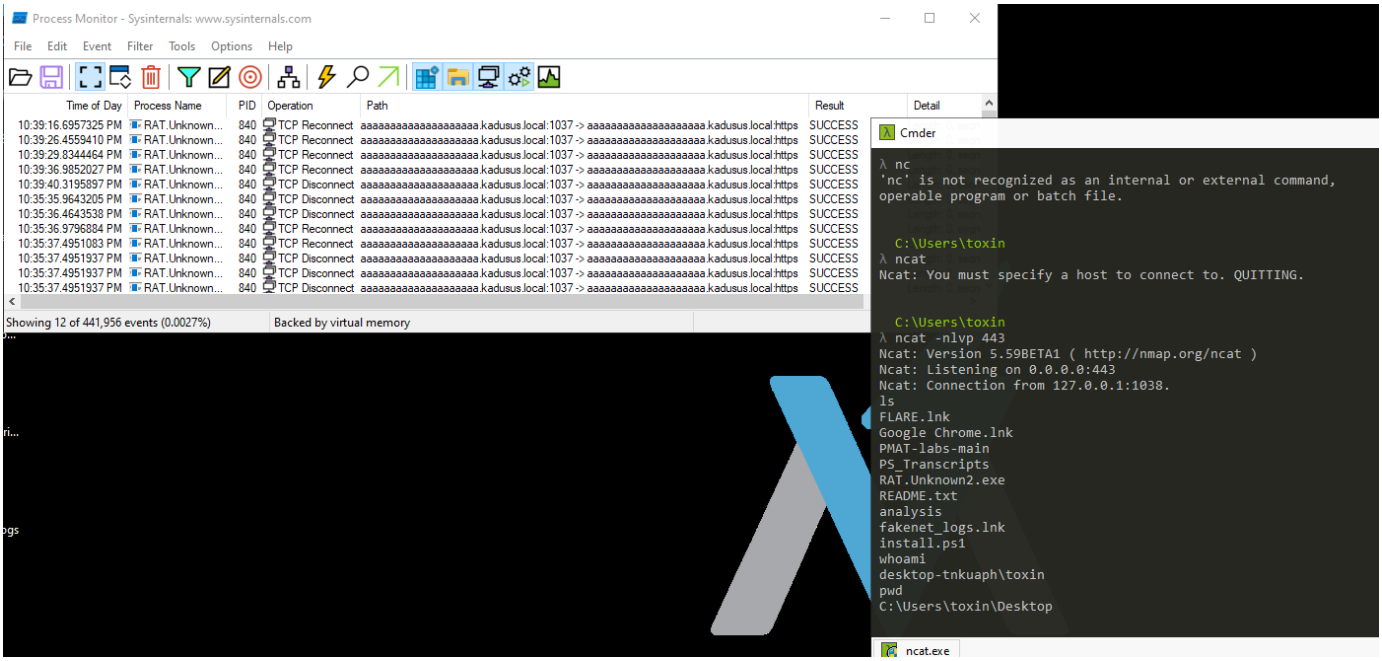


tried DNS: aaaaaaaaaaaaaaaaaaa.kadusus.local

potential call out to specific DNS Record on HTTPS port(443)



Reverse Shell Capability



Conclusion

It's a **REVERSE SHELL** injection malware using DNS