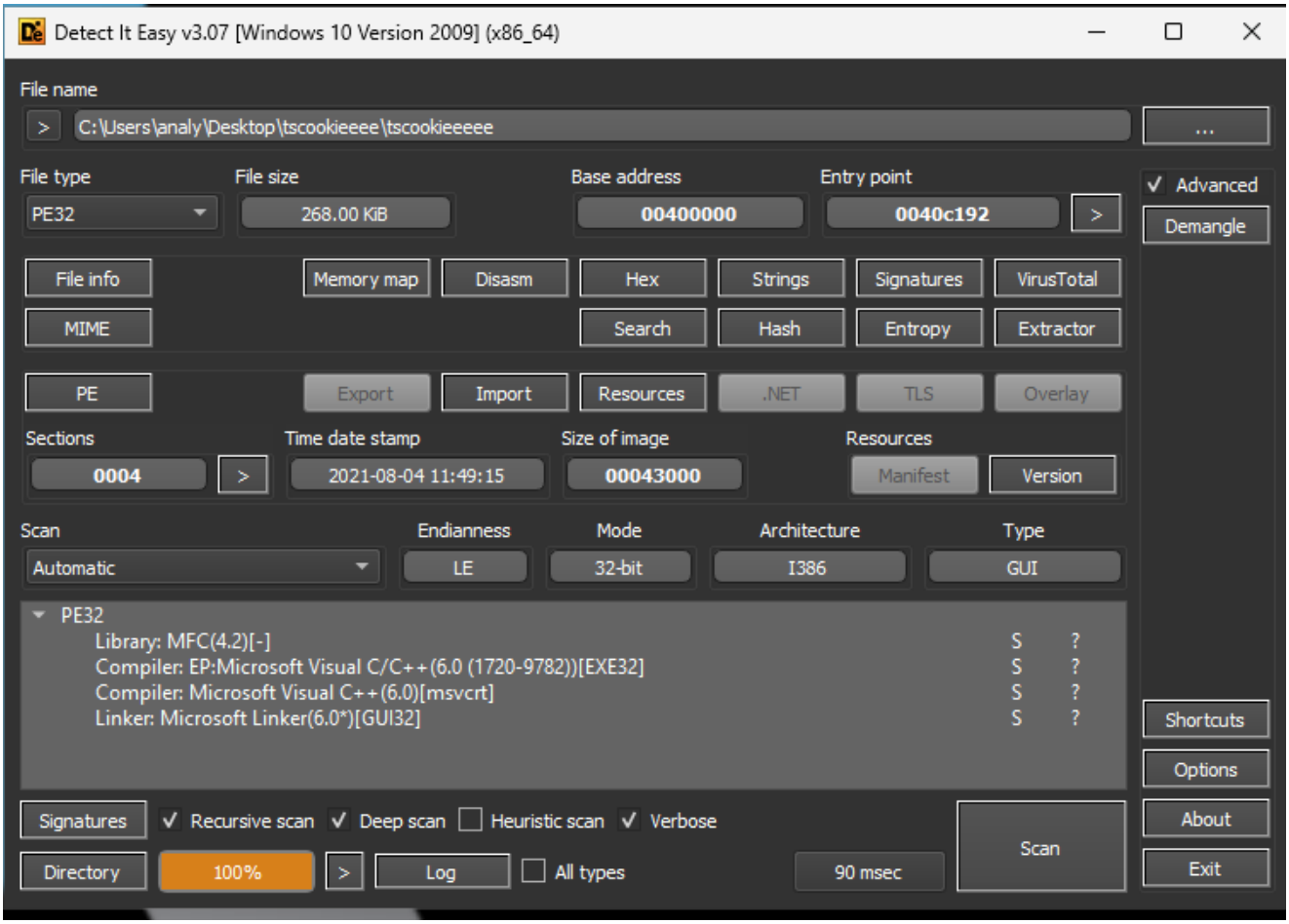
HUI Loader — Malware Analysis Note

medium.com/@morimolymoly/hui-loader-malware-analysis-note-4fa0e1c791d3

morimolymoly August 2, 2023



morimolymoly

--

This note includes brief story of malware variant and my analysis result in my morning coffee time.

HUI Loader is a loader type of malware.

Old HUI Loader has weird string HUIHWASDIHWEIUDHDSFSFEFWEFEWFDSGEFERWGWEEFWFWEWD.

HUI Loader was used by APT10, Blue Termite, A41APT, DEV-0401.

Payload is below.

- PoisonIvy
- PlugX
- Quasar
- SodaMaster
- Cobalt Strike Beacon(Ransomeware ops things by BRONZE STARLIGHT)

I had investigated HUI Loader and links between APT10 and A41APT

I found funny string in the sample.

c:\users\hellokety.ini was embedded to the APT10's PlugX(02b95ef7a33a87cc2b3b6fd47db03e711045974e1ecf631d3ba9e076e1e374e9) and new version of HUI Loader(this was used by A41APT?)

https://twitter.com/cdi_research/status/1635507672417198080

This means A41APT is a sub group of APT10. (everyone know this but clue is important)

HUI Loader fetches encrypted payload from same folder and decrypt and lauch payload. Payload name varies like agent.data, service.dat, svchost.bin etc.

HUI Loader's feature is persistence, security evasion, decrypt and launch payload. Most of them is sometimes not implemented.

We will look at 3ad1a9770a533c2bb8be9d4e7150a2a167d0709c4b0339a5fd6a511008cea7ef to what is implemented!

DLL 64bit and compilation time is so fresh.

DLL has many exports so first I look into cef_api_hash.

Let's look at deeper with Binary Ninja.

It calls one function.

This function looks preparation routine.

This code set agent.data(payload name) to global variable.

It creates thread.

Let's look at this.

FIrst two is a GetProcAddress stuff.

Last one is main code.

HeapAlloc + Decryption + VirtualProtect is a so old technique.

And then, it launches shellcode.

I don’t post full source but it is like a RC4 encryption.

Finally, honestly first, Capa results is here.

HUI Loader is evolved faster.

HUI Loader was used by many threat actors mostly APT10 or APT10-nexus.

Some sample has security evasion, some has interesting string.

In open sourced way, Our most interested one is encrypted payload.

not HUI itself.

References

Analysis of HUI Loader - JPCERT/CC Eyes

To conceal malware's features, attackers sometimes encode the malware and decode it only when they execute it. In such…

blogs.jpcert.or.jp

https://secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader