

## Forum: [Hack Forums](#)

Thread: [\[Malware Analysis\] - MAD RAT BUILDER v7.0](#)

**Bastille** - October 12, 2025, 3:26 am

I stumbled upon a thread a day ago of someone who wanted to sell and share a RAT. The thread has been removed since because OP shared an autobuy link which is not allowed, from the [Help Docs](#).

I saved the thread, links, everything to conduct a malware analysis.

On his website there are "Premium Version" for 20\$ only, and "Free Version". Both of these version have 3 elements :

- MadStealer
- MadRat
- MadMobile (.apk)

I went with MadRat, here is what it looks like after being unzipped :

Python based malware, the "click to install python.exe" file is legit, md5sum = a55e9c1e6421c84a4bd8b4be41492f51

READme.txt :

Code Python 3.10 or above must be installed!

Internet connection must be available!

Disable your antivirus/defender as it might delete some important files!

Run "MadRat.exe"

use the "click to install python.exe" file if you don't have it

use cntrl+v to paste text, and cntrl+c to copy

VT report :

<https://www.virustotal.com/gui/file/c65611e49304db6e5b699e830803f93664c06f9880e8d5d3a6676d18d55a5fa2?nocache=1>

I've ran it throught TRIA.GE, I got many cmd windows popping and disappearing as you can see in the taskbar here :

Checking the TRIA.GE report it's flagged 10 out of 10 : <https://tria.ge/251012-l1ajhssqt5/behavioral1>

Few artifacts :

Code C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference

-ExclusionPath @(\$env:UserProfile, \$env:ProgramData) -ExclusionExtension '.exe' -Force

(obfusctaed)

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE "function  
Local:gZlgUJafynlh{Param([OutputType([Type]])[Parameter(Position=0)][Type[]]\$IGZpHfXmpQWjK  
R,[Parameter(Position=1)][Type]\$hAtUBJlkjY)\$BJiJtWzUpwt=[AppDomain]::CurrentDomain.DefineD  
ynamicAssembly((New-Object Ref

(Uninstalling Windows Malware Removal Tool)

C:\Windows\system32\wusa.exe : wusa /uninstall /kb:890830 /quiet /norestart

Dropped and executed 4 other .exe files :

mad.exe :

<https://www.virustotal.com/gui/file/c40e2c7992be18d3fe8afaa5d163ad8e14f11f3eaa83deb371a68815b864c78d>

pyrdzldsgjog.exe :

<https://www.virustotal.com/gui/file/d23c858c623ca8135ba67e33b3506a9f41b69204f85bff51cd4b3d9fafa7b933>

jwm140.exe :

<https://www.virustotal.com/gui/file/bc6dca56b44335a1adb29c88b2fc0586ff10c6d1b9edd15f75669aa417b5ded>

updater.exe :

<https://www.virustotal.com/gui/file/8172b7e95b87cebfdda01318013e233b21fc395fd8981c775a05c291b1a8620b>

**Nostre** : <https://hackforums.net/member.php?action=profile&uid=5703281>

In case you want to ban, thanks

**Nostre** - October 12, 2025, 4:54 am

Great work as always, [Bastille](#)

**CL1B** - October 12, 2025, 5:10 am

What a weeb.

Thank you for this read and analysis [Bastille](#)

I would love to subscribe to these, would a mega thread be an idea? A thread that you add new analysis too when you do them?

**Bastille** - October 12, 2025, 5:45 am

(Oct 12, 2025 05:10 AM)MarlboroMan Wrote: [\[CITE\]](#) What a weeb.

Thank you for this read and analysis [Bastille](#)

I would love to subscribe to these, would a mega thread be an idea? A thread that you add new analysis too when you do them?

Thanks mate

I already have a mega thread, while I was Staff I was able to edit old threads, but now I can't anymore so I can't add the new analysis, the alternative would be to get the Vendor role but can't afford to spend 150\$ for this

Here is the thread I used to maintain : <https://hackforums.net/showthread.php?tid=6276795>

**CL1B** - October 12, 2025, 5:46 am

Ah ok, I understand..

**MadScientist** - October 24, 2025, 3:46 pm

Awesome work bro, keeping the forums safe! Imagine PAYING someone to infect yourself >.<

**Hackers** - October 26, 2025, 11:39 am

Nice catch, these types of users are becoming more common on HF & other sites where there are lots of devs and people trying indie tools

**JoseMar** - October 26, 2025, 7:52 pm

Nice work my friend, as always.

You know what sucks the most? There are so many people who actually fall for it... For example, look at my last thread about what's happening on YouTube (From long time but 2025 are... insane)

<https://hackforums.net/showthread.php?tid=6312259>

Of course, that so-called LEGIT TOOL fits perfectly with what these hypocrites are doing there.

Nice one.??