

Forum: [Hack Forums](#)

Thread: [Who ACTUALLY owns AegisTools?](#)

Hackers - February 5, 2024, 5:22 am

I recommend you all check this out:

<https://aegistools.pw/landing/manifest.json>

This is [neon_light](#)'s aegis website. A manifest.json file is like the metadata, or package info of a codebase. It's using EVERY RECOVERY...

I know one day soon this link will be offline, or the name will be changed. It's very clear that EveryCrypt/EveryRecovery/etc was then morphed into Aegis Tools.

Here you can see the creator of EveryRecovery contradicting himself in messages to me:

he claims he was just selling some tool for couple of days:

now he admits he made EveryRecovery with a friend:

he denies knowing [neon_light](#) :

he says "maybe" [neon_light](#) stole everyrecovery for aegistools (even though he has never spoke to the guy, never sold everyrecovery, never gave it away, etc):

TR Dropper also partnered up with [youlded - has1](#) to sell everyrecovery
- many profiles have sold everycrypt/recovery/aegistools over last 5+ years

-- Original Post: --

Obviously a lot of evidence has been shared in the dispute against [neon_light](#) (from MrRazor) which essentially proves that at worst, neon is a long-time multi-account scammer, and at best proves that he is lying about having a custom software and is just using a re-skin of another

software caught up in many disputes over the years.

However, there is one last piece to this puzzle: neon_light has sold the exclusive rights to the entire Aegis platform & software, but has continued to sell it. My fear is that neon leaves and then the new buyer just stays here to continue selling Aegis. This has gone on for too long in my opinion. Aegis/EveryCrypt/etc has a long, long history going back 10+ years of being developed, sold, reskinned, etc - with too many scams, disputes, etc to count. Everyone points the finger at the previous owner. I think it's time to say enough is enough. In my opinion, Aegis should be completely banned from being sold, no matter who owns it. It's way too convenient that it gets sold to someone else around the same time as the exit scams start up again. We should stop this cycle of abuse. Sorry Zach Farlow, but the buck needs to stop with you. I don't think you should be allowed to sell this product.

I think we should have an answer - who owns Aegis. Is it Zach, Neon, has1, or someone else?

neon_light claims he sold the software in 2021 here:

[RE: \[10000\\$ in sales\] Selling ownership of Aegistools, online crypter, av scanner, etc](#)

neon_light sells the entire Aegis platform to Zach Farlow on Nov 26, 2023 here:

<https://hackforums.net/contracts.php?action=view&cid=380232>

However neon then gave the Aegis source to MrRazor (and scammed him / didn't deliver the promised product) on Jan 10, 2024 here:

<https://hackforums.net/contracts.php?action=view&cid=382622>

I have not yet received a reply from Zach about this:

MrRazor reached out as well - just seeing this after posting the thread - Zach claims he never received anything:

Since that point, neon has continued to answer new users in convo about selling them more copies of aegis. It seems that Zach Farlow, whether he realizes it or not, has been scammed out of the "full rights to Aegis" as neon continues to sell it. Or Farlow is just another neon multi, or complicit partner? Either way, this software has a decade of shady sales.

If you have no clue what I'm talking about, please review all pages of this thread before asking questions: <https://hackforums.net/showthread.php?tid=6262442>

Jamika - February 7, 2024, 10:51 am

Totally agree with u bro

Np: you r good in investigation, waiting to see omni opinion

Klonopin - February 7, 2024, 11:06 am

After looking into this, this is horrible and I hope this gets looked into..

selling a vb.net crypter from 2012/14 is completely wild.

Good eyes [Hackers](#)

Hackers - February 7, 2024, 9:21 pm

(Feb 7, 2024 12:06 PM)Klonopin Wrote: [\[CITE\]](#) After looking into this, this is horrible and I hope this gets looked into..

selling a vb.net crypter from 2012/14 is completely wild.

Good eyes [Hackers](#)

I found even more.

<https://hackforums.net/showthread.php?tid=5960312>

<https://hackforums.net/showthread.php?tid=4890597>

Hackers - February 15, 2024, 6:07 am

(Feb 7, 2024 10:43 PM)m0hx Wrote: [\[CITE\]](#) now... the next question is.. Is AegisTools.pw the same guy who created AegisCrypter ? (The old AegisCrypter from 2012 era ,-,) it was free and good crypter at the time. [Hackers](#)

for reference:

It was developed in C++. so I don't think he's the same guy :)

Heh, I saw that. I ended up not being able to make any connections besides the name & yeah you're right, all of the crypters I found in my research are .NET

Jacked - February 16, 2024, 3:01 am

Seems to be quite interesting

Hackers - February 27, 2024, 8:37 am

(Feb 16, 2024 04:01 AM)Jacked Wrote: [\[CITE\]](#) Seems to be quite interesting

the plot thickens, I promise you that.

I'll share more when I can :)

jcole - February 27, 2024, 8:46 am

A long awaited investigation that was needed. Props to you [Hackers](#) for digging into this

Hackers - March 22, 2024, 4:47 am

(Feb 16, 2024 04:01 AM)Jacked Wrote: [\[CITE\]](#) Seems to be quite interesting

(Feb 27, 2024 09:37 AM)nodes Wrote: [\[CITE\]](#) the plot thickens, I promise you that.

I'll share more when I can :)

(Feb 27, 2024 09:46 AM)jcole Wrote: [\[CITE\]](#) A long awaited investigation that was needed. Props to you [Hackers](#) for digging into this

I recommend you all check this out:

<https://aegistools.pw/landing/manifest.json>

This is [neon_light](#) 's aegis website. A manifest.json file is like the metadata, or package info of a codebase. It's using EVERY RECOVERY...

I know one day soon this link will be offline, or the name will be changed. It's very clear that EveryCrypt/EveryRecovery/etc was then morphed into Aegis Tools.

Here you can see the creator of EveryRecovery contradicting himself in messages to me:

he claims he was just selling some tool for couple of days:

now he admits he made EveryRecovery with a friend:

he denies knowing [neon_light](#) :

he says "maybe" [neon_light](#) stole everyrecovery for aegistools (even though he has never spoke to the guy, never sold everyrecovery, never gave it away, etc):

Basilisk - April 15, 2024, 5:04 am

Damn, sounds like one of the biggest schemes I've seen, it's crazy how people just fall for that.

Fludems - April 15, 2024, 10:27 am

(Mar 22, 2024 04:47 AM)nodes Wrote: [\[CITE\]](#) [size=x-large]

I recommend you all check this out:

<https://aegistools.pw/landing/manifest.json>

Idk If I've skipped over some context but now it seems like this has been removed and there's a fake seizure notice.

The image doesn't render but look at the HTML LMAO

PHP Code

```
<?php
<div class="container">
  
</div>
```

<https://stats.aegistools.pw/seizurebanner2.jpg>

the banner is just at the root of the web files anyway, this is the actual banner

Oh yeah sorry I didn't realize it was an old post my bad

https://www.google.com/search?q=%22Warning%2C+you+are+entering+a+strictly+monitored+area%22+%26+sca_esv=03235397ee0f049b&sxsrf=ACQVn0_vIRmzTrC1tpHVReUjzzCs9MHJVA%3A1713202215796&ei=J2QdZuaVMP-3hbIP74mB2A8&ved=0ahUKEwimxYDM38SFaxX_W0EAHe9EAPsQ4dUDCBE&uact=5&oq=%22Warning%2C+you+are+entering+a+strictly+monitored+area%22+%26+gs_lp=Egxnd3Mtd2l6LXNlcnAiNiJXYXJuaW5nLCB5b3UgYXJlIGVudGVyaW5nIGEgc3RyaWN0bHkgbW9uaXRvcmlGFyZWElIDIFECEY0AEyBRAhGKABMgUQIRigATIFECEY0AEyBRAhGKABSP8MUAByrwtwAHgBkAEAmAGuAaAB4gOqAQMyLjK4AQPIAQD4AQGYAgSgAvEDWgIIEAAYiQUYogTCAggQABiABBiiBJgDAJIHAzluMqAHmBQ&scient=gws-wiz-serp

There's proof its a fake seizure anyway incase you needed more for whatever reason

InspectorGadget - April 15, 2024, 10:40 am

(Apr 15, 2024 10:27 AM)Onyx Digital Wrote: [\[CITE\]](#) Idk If I've skipped over some context but now it seems like this has been removed and there's a fake seizure notice.

The image doesn't render but look at the HTML LMAO

PHP Code

```
<?php
<div class="container">
    
</div>
```

<https://stats.aegistools.pw/seizurebanner2.jpg>

the banner is just at the root of the web files anyway, this is the actual banner

Oh yeah sorry I didn't realize it was an old post my bad

https://www.google.com/search?q=%22Warning%2C+you+are+entering+a+strictly+monitored+area%22+&sca_esv=03235397ee0f049b&sxsrf=ACQVn0_vIRmzTrC1tpHVReUjzzCs9MHJVA%3A1713202215796&ei=J2QdZuaVMP-3hblP74mB2A8&ved=0ahUKEwimxYDM38SFaX_W0EAHe9EAPsQ4dUDCBE&uact=5&oq=%22Warning%2C+you+are+entering+a+strictly+monitored+area%22+&gs_lp=Egxnd3Mtd2l6LXNlcniAiNiJXYXJuaW5nLCB5b3UgYXJlIGVudGVyaW5nIGEgc3RyaWN0bHkgbW9uaXRvcmlkIGFyZWElDlFECEY0AEyBRAhGKABMgUQIRigATIFECEY0AEyBRAhGKABSP8MUAByrwtwAHgBkAEAmAGuAaAB4gOqAQMyLjK4AQPIAQD4AQGYAgSgAvEDwgIIEAAYiQUYogTCAggQABiABBiiBJgDAJIHAzluMqAHmBQ&scient=gws-wiz-serp

There's proof its a fake seizure anyway incase you needed more for whatever reason

I was getting ready to laugh but actually I think its real. Check this out:

https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2024/Presse2024/240410_PM_Abschaltung_illegaler_Onlineservice.html

Yes it's in German but the fact that they published this would add legitimacy. The fact the German authorities did it might be a useful clue to the nationality of the owner for any curious minds...
SCRATCH THIS, BKA gave their location too!

I've google translated the announcement to English below... Seems the owner was a woman and all their shit has been confiscated, they are in a rough few years.

Spoiler ([Click to View](#))

Illegal online service "AegisTools.pw" shut down

Suspected operator identified +++ Platform enabled concealment of malware software and theft of access data

The Koblenz Public Prosecutor's Office – State Central Office for Cybercrime (LZC) – and the Federal

Criminal Police Office (BKA) shut down the illegal online service "AegisTools.pw" on April 9th, 2024. A German citizen is suspected of operating a business on a commercial basis.

a criminal trading platform on the Internet. In this context, searches were carried out Security measures at the alleged operator's residential property in Speyer, Rhineland-Palatinate.

Numerous pieces of evidence were seized, including several PCs and laptops, various data carriers and cell phones.

"AegisTools.pw" has been known in the underground economy since 2020

Platform that primarily provided counter antivirus and crypting services – two out

From a phenomenological point of view, they are important pillars within the cybercrime-as-a-service model. She made it possible to disguise malware so that it could be detected by common antivirus programs could not be recognized. "Aegis Tools.pw" also offered tests directly on the platform Checking the effectiveness of the encryption. Furthermore, software was developed for the un-Permitted acquisition of user password access data is offered. "AegisTools.pw" itself gen did not require its users to register in the traditional way and was able to operate almost anonymously.

be applied. The police evaluations indicate that the platform is in use has been used by over 1,000 users worldwide for their cybercriminal activities. was taken. All services could be paid for with cryptocurrencies.

The shutdown of "AegisTools.pw" and the identification of the suspected operator are followed with the participation of national and international partners - including the US Canadian FBI, the Western District of North Carolina (WDNC) US Attorney's Office, the computers Crime and Intellectual Property Section of the US Department of Justice and the Rhineland-Palatinate

cial police – and are another blow against specialized cybercrime actors in the underground economy.

The following security banner was published on the platform's website:
No further information can be provided at this time

Fludems - April 15, 2024, 12:19 pm

(Apr 15, 2024 10:40 AM)InspectorGadget Wrote: [\[CITE\]](#) I was getting ready to laugh but actually I think its real. Check this out:
https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2024/Presse2024/240410_PM_Abschaltung_illegaler_Onlineservice.html

Yes it's in German but the fact that they published this would add legitimacy. The fact the german authorities did it might be a useful clue to the nationality of the owner for any curious minds...
SCRATCH THIS, BKA gave their location too!

I've google translated the announcement to English below... Seems the owner was a woman and all their shit has been confiscated, they are in a a rough few years.

Spoiler [\(Click to View\)](#)

Illegal online service "AegisTools.pw" shut down
Suspected operator identified +++ Platform enabled concealment of malware software and theft of access data
The Koblenz Public Prosecutor's Office – State Central Office for Cybercrime (LZC) – and the Federal Criminal Police Office (BKA) shut down the illegal online service "AegisTools.pw" on April 9th, 2024. tet. A German citizen is suspected of operating a business on a commercial basis. a criminal trading platform on the Internet. In this context, searches were carried out Security measures at the alleged operator's residential property in Speyer, Rhineland-Palatinate. Numerous pieces of evidence were seized, including several PCs and laptops, various data carriers and cell phones.

"AegisTools.pw" has been known in the underground economy since 2020
Platform that primarily provided counter antivirus and crypting services – two out
From a phenomenological point of view, they are important pillars within the cybercrime-as-a-service model. She made it possible to disguise malware so that it could be detected by common antivirus programs could not be recognized. "Aegis Tools.pw" also offered tests directly on the platform

Checking the effectiveness of the encryption. Furthermore, software was developed for the un-Permitted acquisition of user password access data is offered. "AegisTools.pw" itself gen did not require its users to register in the traditional way and was able to operate almost anonymously.

be applied. The police evaluations indicate that the platform is in use has been used by over 1,000 users worldwide for their cybercriminal activities. was taken. All services could be paid for with cryptocurrencies.

The shutdown of "AegisTools.pw" and the identification of the suspected operator are followed with the participation of national and international partners - including the US Canadian FBI, the Western District of North Carolina (WDNC) US Attorney's Office, the computers Crime and Intellectual Property Section of the US Department of Justice and the Rhineland-Palatinate

cial police – and are another blow against specialized cybercrime actors in the underground economy.

The following security banner was published on the platform's website:

No further information can be provided at this time

Sorry I may just be being an idiot, it happens quite often haha

But what made me believe it was a fake seizure was this:

alt="Warning, you are entering a strictly monitored area"

The alt text mismatches what the purpose the image actually serves, and it looks like it's just a template has been used

I think this is a copy of a true seizure page, but I'm not entirely sure:

https://github.com/Linuzifer/domain_seizure/blob/master/bka/index.html

But the html is a lot different anyway

EDIT: Nah there is publications saying a seizure took place I'm probably wrong my bad

Zach_Farlow - September 3, 2024, 12:21 pm

Cant believe i am just now seeing this. But yes i was scammed as i did not do enough research on this.

Tyr - November 18, 2025, 9:06 am

(Sep 3, 2024 12:21 PM)Zach_Farlow Wrote: [\[CITE\]](#) Cant believe i am just now seeing this. But yes i was scammed as i did not do enough research on this.

Ditto. Thanks for posting this.