

Forum:[Hack Forums](#)

Thread: [U.S. DoJ Dismantles Warzone RAT Infrastructure, Arrests Key Operators](#)

DI?E - February 12, 2024, 9:58 am

The U.S. Justice Department (DoJ) on Friday announced the seizure of online infrastructure that was used to sell a remote access trojan (RAT) called Warzone RAT.

The domains – [www.warzone\[.\]ws](#) and three others – were "used to sell computer malware used by cybercriminals to secretly access and steal data from victims' computers," the DoJ said.

Alongside the takedown, the international law enforcement effort has arrested and indicted two individuals in Malta and Nigeria for their involvement in selling and supporting the malware and helping other cybercriminals use the RAT for malicious purposes.

The defendants, Daniel Meli (27) and Prince Onyeoziri Odinakachi (31) have been charged with unauthorized damage to protected computers, with the former also accused of "illegally selling and advertising an electronic interception device and participating in a conspiracy to commit several computer intrusion offenses."

Meli is alleged to have offered malware services at least since 2012 through online hacking forums, sharing e-books, and helping other criminals use RATs to carry out cyber attacks. Prior to Warzone RAT, he had sold another RAT known as Pegasus RAT.

Like Meli, Odinakachi also provided online customer support to purchasers of Warzone RAT malware between June 2019 and no earlier than March 2023. Both individuals were arrested on February 7, 2024.

Warzone RAT, also known as Ave Maria, was first documented by Yoroi in January 2019 as part of a cyber attack targeting an Italian organization in the oil and gas sector towards the end of 2018 using phishing emails bearing bogus Microsoft Excel files exploiting a known security flaw in the Equation Editor (CVE-2017-11882).

Sold under the malware-as-a-service (Maas) model for \$38 a month (or \$196 for a year), it functions as an information stealer and facilitates remote control, thereby allowing threat actors to commandeer the infected hosts for follow-on exploitation.

Some of the notable features of the malware include the ability to browse victim file systems, take screenshots, record keystrokes, steal victim usernames and passwords, and activate the computer's webcams without the victim's knowledge or consent.

"Ave Maria attacks are initiated via phishing emails, once the dropped payload infects the victim's machine with the malware, it establishes communication with the attacker's command-and-control (C2) server on non-HTTP protocol, after decrypting its C2 connection using RC4 algorithm," Zscaler ThreatLabz said in early 2023.

On one of the now-dismantled websites, which had the tagline "Serving you loyally since 2018," the developers of the C/C++ malware described it as reliable and easy to use. They also provided the ability for customers to contact them via email ([solmyr@warzone\[.\]ws](#)), Telegram ([@solwz](#) and [@sammysamwarzone](#)), Skype ([vuln.hf](#)), as well as via a dedicated "client area."

An additional contact avenue was Discord, where the users were asked to get in touch with an account with the ID Meli#4472. Another Telegram account linked to Meli was @daniel96420.

Outside of cybercrime groups, the malware has also been put to use by several advanced threat actors like YoroTrooper as well as those associated with Russia over the past year.

The DoJ said the U.S. Federal Bureau of Investigation (FBI) covertly purchased copies of Warzone RAT and confirmed its nefarious functions. The coordinated exercise involved assistance from authorities in Australia, Canada, Croatia, Finland, Germany, Japan, Malta, the Netherlands, Nigeria, Romania, and Europol.

webdev77 - February 12, 2024, 10:05 am

Here's the reminder out there for any noobs that "For educational use only" is not a valid defense if you are selling a product that is clearly for nefarious purposes.

Omniscient - February 12, 2024, 11:06 am

I'd like to read the actual DoJ documents about this and read the indictment. Seems to be from a Grand Jury and likely sealed. btw, some discussion of the this goes on in Convo.

HALx86 - February 12, 2024, 11:14 am

I feel like the DoD/DoJ has really ramped up their seizure game. I wonder if they just got more efficient or if they're unraveling some kind of nest that leads them to the next one.

Omniscient - February 12, 2024, 11:17 am

(Feb 12, 2024 12:14 PM)HALx86 Wrote: [\[CITE\]](#) I feel like the DoD/DoJ has really ramped up their seizure game. I wonder if they just got more efficient or if they're unraveling some kind of nest that leads them to the next one.

Seems about the same to me and I'm paying attention for 17 years.

DI?E - February 12, 2024, 11:33 am

(Feb 12, 2024 12:06 PM)Omniscient Wrote: [\[CITE\]](#) I'd like to read the actual DoJ documents about this and read the indictment. Seems to be from a Grand Jury and likely sealed. btw, some discussion of the this goes on in Convo.

Seeing as they just got hit I'm sure it won't be long before all that is released.

Joel - February 12, 2024, 11:59 am

Seems like its legal to use the software but not to sell it, when it really should be the opposite. Has there been any arrests made on people USING the software besides the creators?

webdev77 - February 12, 2024, 12:02 pm

(Feb 12, 2024 12:59 PM)Joel Wrote: [\[CITE\]](#) Seems like its legal to use the software but not to sell it, when it really should be the opposite. Has there been any arrests made on people USING the software besides the creators?

The answer is neither. It's just easier to go after the seller. Some Blackshades customers were charged almost a decade ago.

<https://www.justice.gov/usao-sdny/video/charges-announced-con-blackshades-malware-enabled-use-rs-secretly-control-computers>

Quote:Kyle Fedorek, who purchased the RAT and used it to steal online account information from hundreds of victims; and Marlen Rappa, who purchased the RAT and used it to spy on dozens of victims and steal online account information.

neightworks. - February 12, 2024, 12:58 pm

(Feb 12, 2024 01:02 PM)webdev77 Wrote: [\[CITE\]](#) The answer is neither. It's just easier to go after the seller. Some Blackshades customers were charged almost a decade ago.

<https://www.justice.gov/usao-sdny/video/charges-announced-con-blackshades-malware-enabled-use-rs-secretly-control-computers>

Not just some, every single user that paid with PayPal which was hundreds if not thousands got a knock.

Which reminds me wasn't the actual reason BS got taken so serious is that a forum member here infected multiple female celebs?

Popular - February 12, 2024, 1:14 pm

(Feb 12, 2024 11:05 AM)webdev77 Wrote: [\[CITE\]](#) Here's the reminder out there for any noobs that "For educational use only" is not a valid defense if you are selling a product that is clearly for nefarious purposes.

So true. People type that 1 liner all day long and think they're covered. ?

Joel - February 12, 2024, 1:23 pm

(Feb 12, 2024 01:58 PM)neightworks. Wrote: [\[CITE\]](#) Not just some, every single user that paid with PayPal which was hundreds if not thousands got a knock.

Which reminds me wasn't the actual reason BS got taken so serious is that a forum member here infected multiple female celebs?

I'd say the people buying a RAT with PayPal probably werent using it to its full potential anyway.

neightworks. - February 12, 2024, 1:42 pm

(Feb 12, 2024 02:23 PM)Joel Wrote: [\[CITE\]](#) I'd say the people buying a RAT with PayPal probably werent using it to its full potential anyway.

Idk fam those days you could get FUD for like \$2 and everyone and their dad tried to get RuneScape cheats.

illuminati? - February 12, 2024, 2:12 pm

(Feb 12, 2024 01:58 PM)neightworks. Wrote: [\[CITE\]](#) Which reminds me wasn't the actual reason BS got taken so serious is that a forum member here infected multiple female celebs?

That and their stealer that they were selling was on a god tier for that time period.

LEGENDAVIE - February 12, 2024, 4:01 pm

"the FBI covertly purchased and analyzed the Warzone RAT malware, confirming its multiple malicious functions"

Wonder if they left positive B-rating ?

DI?E - February 13, 2024, 1:26 am

(Feb 12, 2024 05:01 PM)LEGENDAVIE Wrote: [\[CITE\]](#) "the FBI covertly purchased and analyzed the Warzone RAT malware, confirming its multiple malicious functions"

Wonder if they left positive B-rating ?

Good one. ?

(Feb 12, 2024 02:23 PM)Joel Wrote: [\[CITE\]](#) I'd say the people buying a RAT with PayPal probably weren't using it to its full potential anyway.

Even if you bought it with crypto they seized the licensing servers. It is game over. You really trust a RAT seller to not log IP addresses for verification these days? It is a cash grab and that is how they get caught (the users of said product).

Blackshades, Orcus, LuminosityLink, NanoCore etc. Same pattern.

Mercury - February 13, 2024, 5:41 am

Frankly, I'm shocked that Warzone survived as long as it did. I've never used it and cannot speak to the quality of it, but it seemed to be around for quite a long time. I can only imagine the level of exposure it had. It's always disappointing when these guys get hit, but man I can't say I'm surprised.