Avaddon ransomware operation shuts down and releases decryption keys

therecord.media/avaddon-ransomware-operation-shuts-down-and-releases-decryption-keys/

June 11, 2021

The criminal group behind the Avaddon ransomware has shut down its operation today and released decryption keys for past victims.

The keys were made available earlier today via a private message sent to Bleeping Computer, a ransomware support forum and news site that has been covering the ransomware scene since 2016.

The keys have now been shared with Emsisoft, a security firm that has previously released tens of free decryption utilities for all kinds of ransomware strains.

The company expects to release a free decryptor over the weekend, Emsisoft security researcher Michael Gillespie has told *The Record* in an interview. [*Update: Decryptor now live here*.]

The decryptor will take the 2,934 decryption keys and allow past Avaddon victims to decrypt their files for free if they still have the encrypted files around and have not deleted the data.

> PSA: Avaddon appears to have shut down and released 2934 private keys of victims. A public Emsisoft decryption tool is coming soon. Do not pay. If you are a victim and want to know if your files can be decrypted, please reach out to Thanks.
>
> — Fabian Wosar (@fwosar) June 11, 2021

Avaddon was slowly becoming a top-tier threat

The Avaddon shutdown today came out of the blue and has surprised the security research community.

After the disappearance of the Darkside ransomware gang in the aftermath of the Colonial Pipeline attack, the Avaddon gang had moved very aggressively to fill the gap left on the market, Allan Liska, a Recorded Future security analyst who tracks ransomware operations, told *The Record*.

“Avaddon was tied with Conti for most number of ransomware extortions published since the Colonial Pipeline attack,” Liska told us. “Fifty-nine victims published since May 7th), 182 in total since launching in August 2020.”

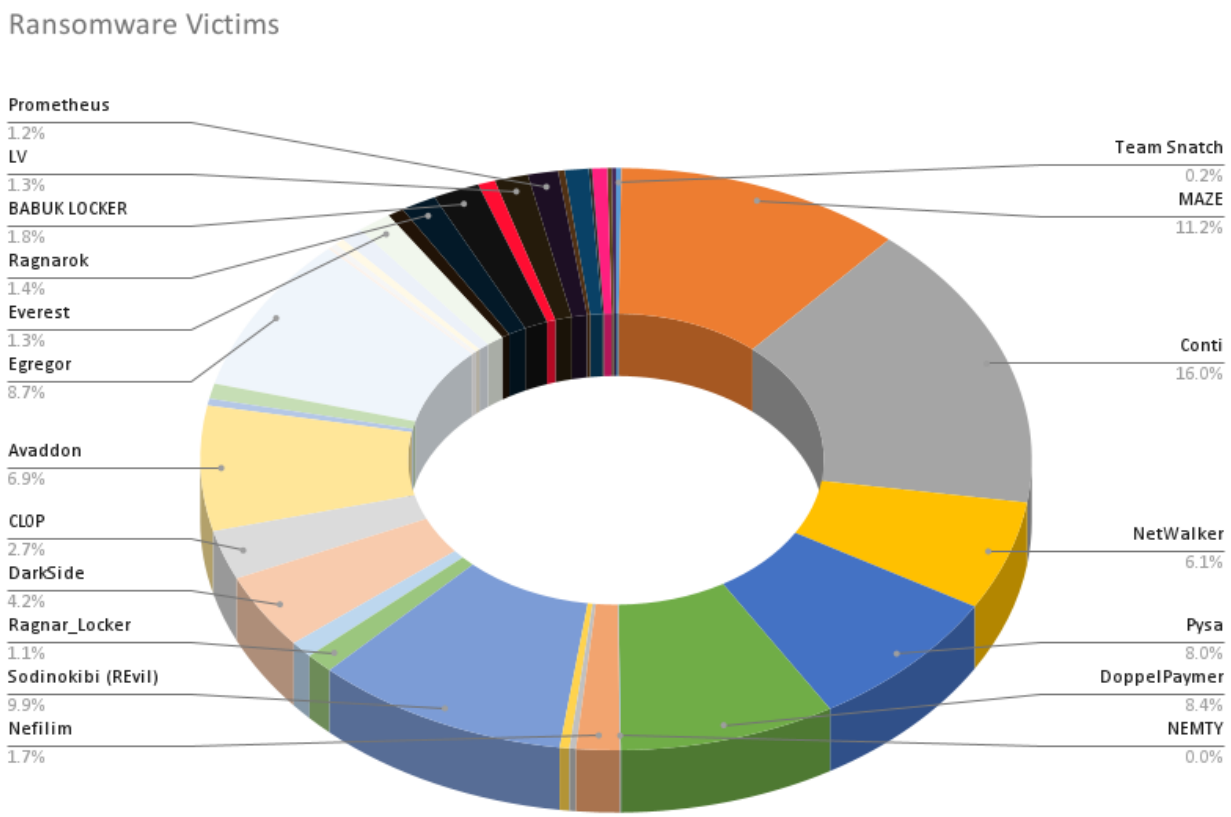
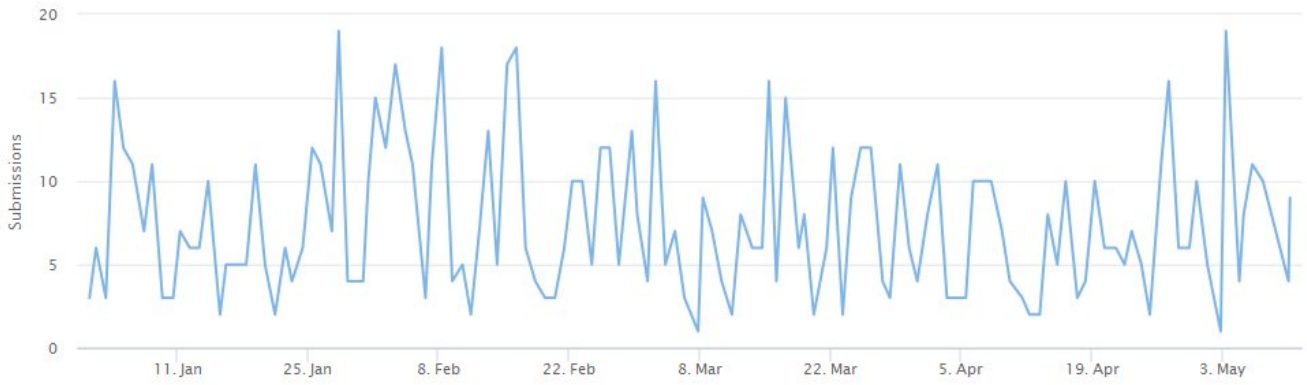


Image: Recorded Future

Furthermore, the group had also been extremely active even before the Colonial Pipeline attack.

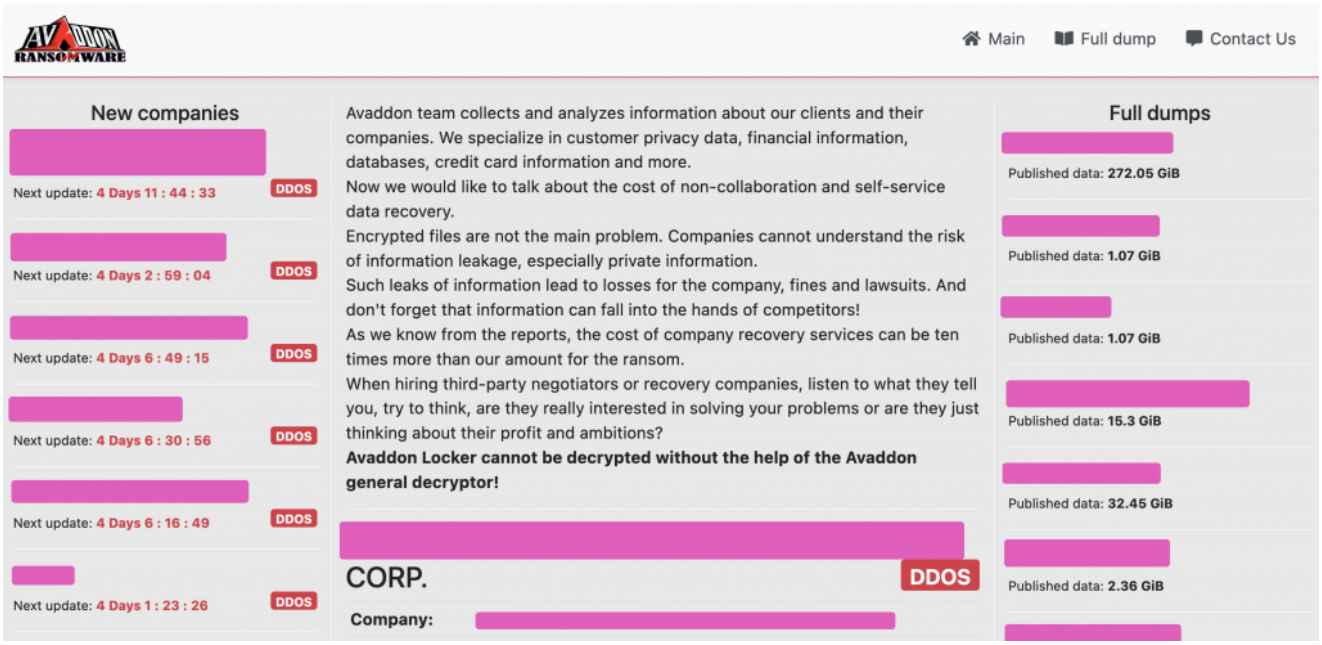
Tens of victims reported intrusions and submitting Avaddon-encrypted files and ransom notes to the ID-Ransomware service on an almost weekly basis this year.



Avaddon's recent sudden spike in attacks also led the US Federal Bureau of Investigation and the Australian Cyber Security Centre to issue alerts at the start of May about their ever-growing number of intrusions.

Actual shutdown or just rebranding?

However, earlier today, the gang shut down its servers, its dark web leak site, wiped profiles on hacking forums, and then sent the decryption keys to Bleeping Computer.



Avaddon ransomware leak site

Unlike other ransomware gangs who shut down operations through pompous messages posted online, the Avaddon gang appears to have disappeared from the face of the earth.

Messages to a now-wiped hacking forum account were not returned. All posts made from that account have also been deleted.

A theory gaining ground in the infosec community suggests that the group may be entering a rebranding phase, something that many other gangs have done before, such as Nemty-to-Nefilim and Gandcrab-to-REvil.

Shortly after the Colonial Pipeline attack, the Avaddon gang also announced plans to go private and work only with a selected number of affiliates for their intrusions.

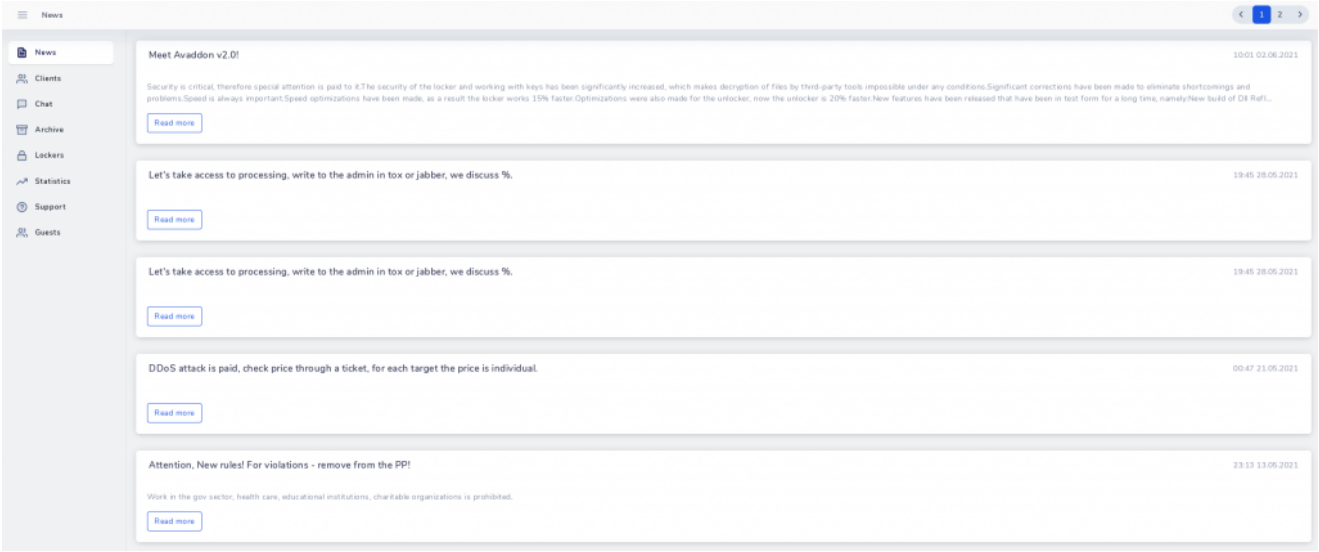
Rebranding and going private would be a good way for the Avaddon gang to lose the law enforcement agencies and security firms currently tracking its every moves.

> @ddd1ms & @campuscodi Some change is happening…. @Raj_Samani @ChristiaanBeek @McAfee_Labs pic.twitter.com/SIgNW3V2Df
>
> — John Fokker (@John_Fokker) May 14, 2021

Prior to shutting down, the Avaddon gang was also notorious for running one of the most professional and responsive Ransomware-as-a-Service (RaaS) operations.

The group advertised through hacking forums such as Exploit and XSS, was responsive to customer demands, and ran an automated leak portal as a double-extortion scheme for victims who refused to pay.

In addition, the Avaddon gang also built one of the easier to use RaaS portals (see image below, courtesy of the Recorded Future Insikt Group), and when a bug was found in its code that allowed for free decryptions, they fixed it within a day.



Avaddon RaaS backend panel

Tags

- Avaddon
- cybercrime
- RaaS
- Ransomware
- shutdown

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.