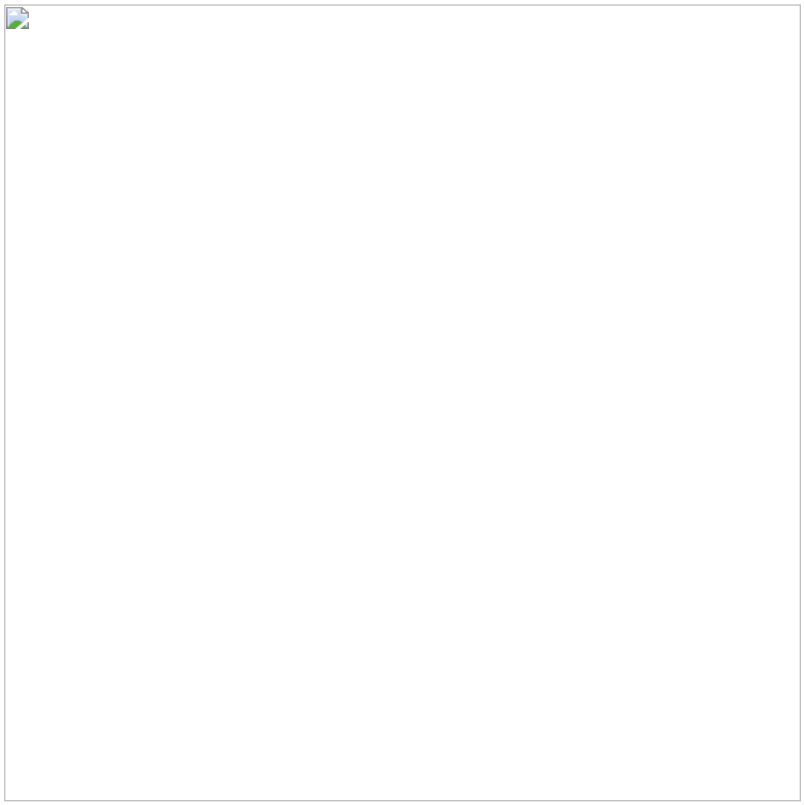
Orcus RAT Author Charged in Malware Scheme

krebsonsecurity.com/2019/11/orcus-rat-author-charged-in-malware-scheme

In July 2016, KrebsOnSecurity published a story identifying a Toronto man as the author of the **Orcus RAT**, a software product that's been marketed on underground forums and used in countless malware attacks since its creation in 2015. This week, Canadian authorities criminally charged him with orchestrating an international malware scheme.



An advertisement for Orcus RAT.

The accused, 36-year-old **John "Armada" Revesz**, has maintained that Orcus is a legitimate "**R**emote **A**dministration **T**ool" aimed at helping system administrators remotely manage their computers, and that he's not responsible for how licensed customers use his product.

In my 2016 piece, however, several sources noted that Armada and his team were marketing it more like a **R**emote **A**ccess **T**rojan, providing ongoing technical support and help to customers who'd purchased Orcus but were having trouble figuring out how to infect new machines or hide their activities online.

Follow-up reporting revealed that the list of features and plugins advertised for Orcus includes functionality that goes significantly beyond what one might see in a traditional remote administration tool, such as DDoS-for-hire capabilities, and the ability to disable the light indicator on webcams so as not to alert the target that the RAT is active.

Canadian investigators don't appear to be buying Revesz' claims. On Monday the **Royal Canadian Mounted Police** (RCMP) announced it had charged Revesz with operating an international malware distribution scheme under the company name "Orcus Technologies."

"An RCMP criminal investigation began in July 2016 after reports of a significant amount of computers were being infected with a 'Remote Access Trojan' type of virus," the agency said in a statement.

The RCMP filed the charges eight months after executing a search warrant at Revesz' home, where they seized several hard drives containing Orcus RAT customer names, financial transactions, and other information.

"The evidence obtained shows that this virus has infected computers from around the world, making thousands of victims in multiple countries," the RCMP said.

Revesz did not respond to requests for comment.

If Revesz's customers are feeling the heat right now, they probably should be. Several former customers of his took to Hackforums[.]net to complain about being raided by investigators who are trying to track down individuals suspected of using Orcus to infect computers with malware.

"I got raided [and] within the first 5 minutes they mention Orcus to me," complained one customer on Hackforums[.]net, the forum where Revesz principally advertised his software. That user pointed to a March 2019 media advisory released by the **Australian Federal Police**, who said they'd executed search warrants there as part of an investigation into RAT technology conducted in tandem with the RCMP.

According to Revesz himself, the arrests and searches related to Orcus have since expanded to individuals in the United States and Germany.

The sale and marketing of remote administration tools is not illegal in the United States, and indeed there are plenty such tools sold by legitimate companies to help computer experts remotely administer computers.

However, these tools tend to be viewed by prosecutors as malware and spyware when their proprietors advertise them as hacking devices and provide customer support aimed at helping buyers deploy the RATs stealthily and evade detection by anti-malware programs.

Last year, a 21-year-old Kentucky man pleaded guilty to authoring and distributing a popular hacking tool called "LuminosityLink," which experts say was used by thousands of customers to gain access to tens of thousands of computers across 78 countries worldwide.

Also in 2018, 27-year-old Arkansas resident **Taylor Huddleston** was sentenced to three years in jail for making and selling the “NanoCore RAT,” which was being used to spy on webcams and steal passwords from systems running the software.

In many previous law enforcement investigations targeting RAT developers and sellers, investigators also have targeted customers of these products. In 2014, the U.S. Justice Department announced a series of actions against more than 100 people accused of purchasing and using “Blackshades,” a cheap and powerful RAT that the U.S. government said was used to infect more than a half million computers worldwide.

It’s remarkable how many denizens of various hacking forums persist in believing that an end-user licensing agreement (EULA) or “terms of service” (TOS) disavowing any responsibility for what customers do with the product somehow absolves sellers of RAT programs of any liability when they then turn around and actively assist customers in using the tools to infect systems with malware.