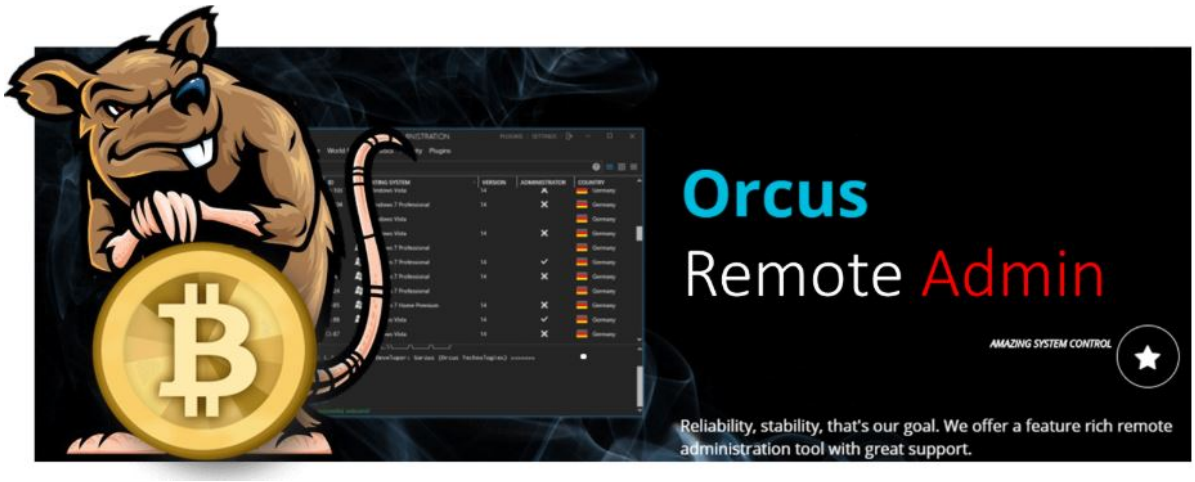
Canadian Police Raid 'Orcus RAT' Author

krebsonsecurity.com/2019/04/canadian-police-raid-orcus-rat-author/

Canadian police last week raided the residence of a Toronto software developer behind "**Orcus RAT**," a product that's been marketed on underground forums and used in countless malware attacks since its creation in 2015. Its author maintains Orcus is a legitimate **R**emote **A**dministration **T**ool that is merely being abused, but security experts say it includes multiple features more typically seen in malware known as a **R**emote **A**ccess **T**rojan.



An advertisement for Orcus RAT.

As first detailed by KrebsOnSecurity in July 2016, Orcus is the brainchild of **John "Armada" Revesz**, a Toronto resident who until recently maintained and sold the RAT under the company name **Orcus Technologies**.

In an "official press release" posted to pastebin.com on Mar. 31, 2019, Revesz said his company recently was the subject of an international search warrant executed jointly by the **Royal Canadian Mounted Police** (RCMP) and the **Canadian Radio-television and Telecommunications Commission** (CRTC).

"In this process authorities seized numerous backup hard drives [containing] a large portion of Orcus Technologies business, and practices," Revesz wrote. "Data inclusive on these drives include but are not limited to: User information inclusive of user names, real names, financial transactions, and further. The arrests and searches expand to an international investigation at this point, including countries as America, Germany, Australia, Canada and potentially more."

Reached via email, Revesz declined to say whether he was arrested in connection with the search warrant, a copy of which he shared with KrebsOnSecurity. In response to an inquiry from this office, the RCMP stopped short of naming names, but said "we can confirm that our

National Division Cybercrime Investigative Team did execute a search warrant at a Toronto location last week."

The RCMP said the raid was part of an international coordinated effort with the Federal Bureau of Investigation and the Australian Federal Police, as part of "a series of ongoing, parallel investigations into Remote Access Trojan (RAT) technology. This type of malicious software (malware) enables remote access to Canadian computers, without their users' consent and can lead to the subsequent installation of other malware and theft of personal information."

"The CRTC executed a warrant under Canada's Anti-Spam Legislation (CASL) and the RCMP National Division executed a search warrant under the Criminal Code respectively," reads a statement published last week by the Canadian government. "Tips from international private cyber security firms triggered the investigation."

Revesz maintains his software was designed for legitimate use only and for system administrators seeking more powerful, full-featured ways to remotely manage multiple PCs around the globe. He's also said he's not responsible for how licensed customers use his products, and that he actively kills software licenses for customers found to be using it for online fraud.

Yet the list of features and plugins advertised for this RAT 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.

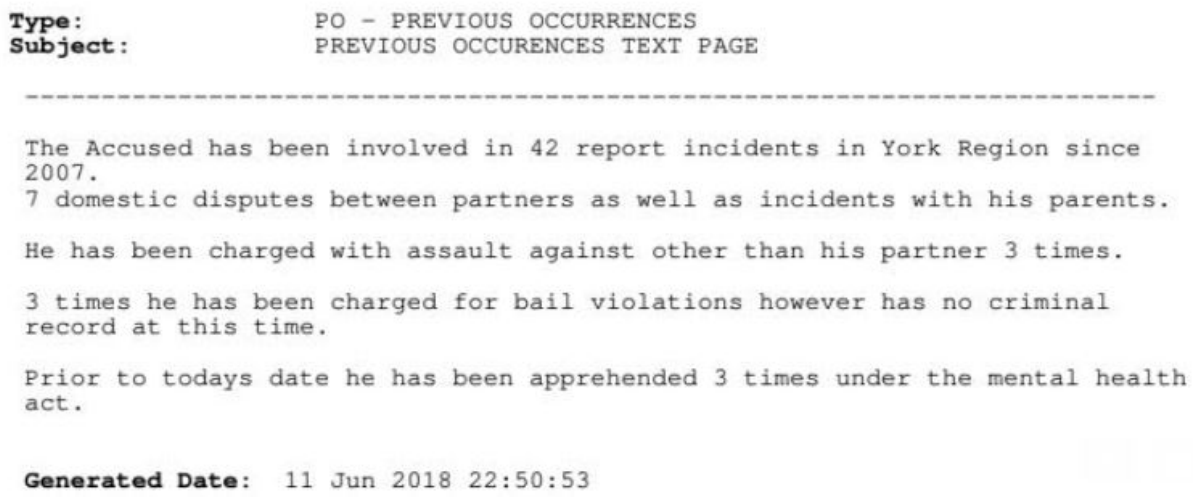
"It can also implement a watchdog that restarts the server component or even trigger a Blue Screen of Death (BSOD) if the someone tries to kill its process," wrote researchers at security firm Fortinet in a Dec. 2017 analysis of the RAT. "This makes it harder for targets to remove it from their systems. These are, of course, on top of the obviously ominous features such as password retrieval and key logging that are normally seen in Remote Access Trojans."

As KrebsOnSecurity noted in 2016, in conjunction with his RAT Revesz also sold and marketed a bulletproof "dynamic DNS service" that promised not to keep any records of customer activity.

Revesz appears to have a flair for the dramatic, and has periodically emailed this author over the years. Sometimes, the missives were taunting, or vaguely ominous and threatening. Like the time he reached out to say he was hiring a private investigator to find and track me. Still other unbidden communications from Revesz were friendly, even helpful with timely news tips.

According to Revesz himself, he is no stranger to the Canadian legal system. In June 2018, Revesz shared court documents indicating he has been involved in multiple physical assault charges since 2007, including “7 domestic disputes between partners as well as incidents with his parents.”

“I am not your A-typical computer geek, Brian,” he wrote in a 2018 email. “I tend to have a violent nature, and have both Martial arts and Military training. So, I suppose it is really good that I took your article with a grain of salt instead of actually really getting upset.”



Type: PO - PREVIOUS OCCURRENCES
Subject: PREVIOUS OCCURENCES TEXT PAGE

The Accused has been involved in 42 report incidents in York Region since 2007.
7 domestic disputes between partners as well as incidents with his parents.

He has been charged with assault against other than his partner 3 times.

3 times he has been charged for bail violations however has no criminal record at this time.

Prior to todays date he has been apprehended 3 times under the mental health act.

Generated Date: 11 Jun 2018 22:50:53

The sale and marketing of remote administration tools is not illegal in the United States, and indeed there are plenty of 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.

Earlier this year, Revesz posted on Twitter that he was making the source code for Orcus RAT publicly available, and focusing his attention on developing a new and improved RAT product.

Meanwhile on Hackforums[.]net — the forum where Orcus was principally advertised and sold — members and customers expressed concern that authorities would soon be visiting Orcus RAT customers, posts that were deleted almost as quickly by the Hackforums administrator.

As if in acknowledgement of that concern, in the Pastebin press release published this week Revesz warned people away from using Orcus RAT, and added some choice advice for others who would follow his path.

“Orcus is no longer to be considered safe or secure solution to Remote Administrative needs,” he wrote, pointing to a screenshot of a court order he says came from one of the police investigators, which requires him to abstain from accessing Hackforums or Orcus-related sites. “Please move away from this software without delay. It has been a pleasure getting to know everyone in my time online, and I hope you all can take my words as a life lesson. Stay safe, don’t do stupid shit.”