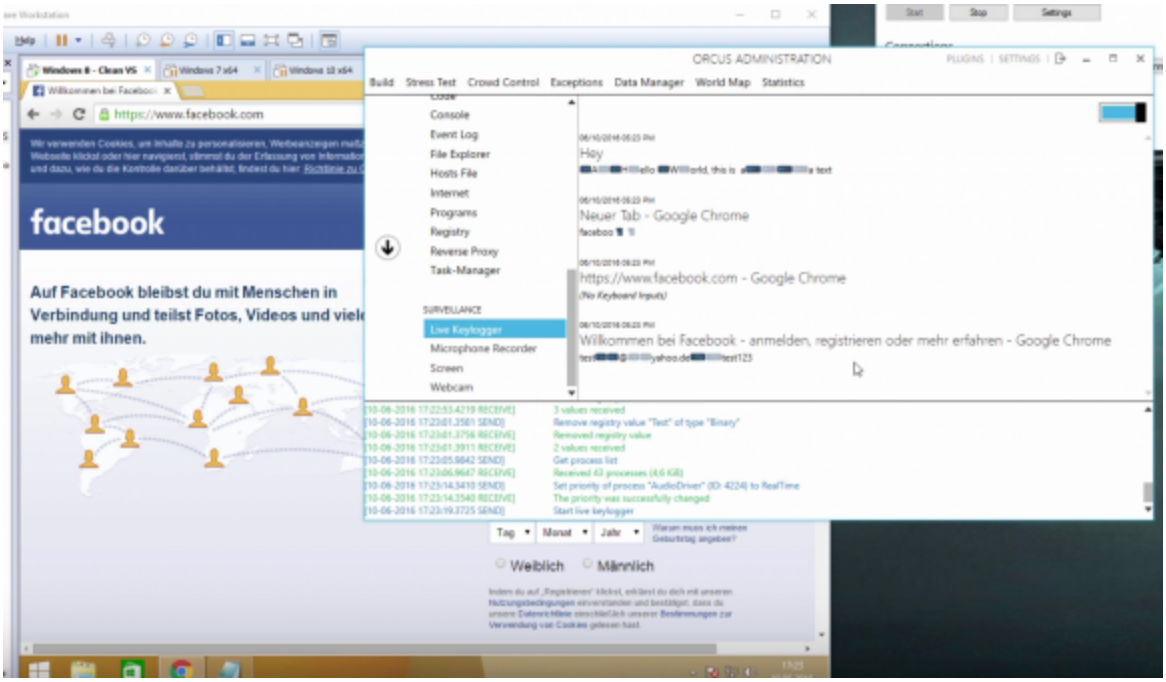
Canadian Man Behind Popular ‘Orcus RAT’

krebsonsecurity.com/2016/07/canadian-man-is-author-of-popular-orcus-rat/

Far too many otherwise intelligent and talented software developers these days apparently think they can get away with writing, selling and supporting malicious software and then couching their commerce as a purely legitimate enterprise. Here’s the story of how I learned the real-life identity of Canadian man who’s laboring under that same illusion as proprietor of one of the most popular and affordable tools for hacking into someone else’s computer.

Earlier this week I heard from Daniel Gallagher, a security professional who occasionally enjoys analyzing new malicious software samples found in the wild. Gallagher said he and members of @malwrhunterteam and @MalwareTechBlog recently got into a Twitter fight with the author of **Orcus RAT,** a tool they say was explicitly designed to help users remotely compromise and control computers that don’t belong to them.



A still frame from a Youtube video demonstrating Orcus RAT’s keylogging ability to steal passwords from Facebook and other sites.

The author of Orcus — a person going by the nickname “Ciriis Mcgraw” a.k.a. “Armada” on Twitter and other social networks — claimed that his RAT was in fact a benign “remote administration tool” designed for use by network administrators and not a “remote access Trojan” as critics charged. Gallagher and others took issue with that claim, pointing out that they were increasingly encountering computers that had been infected with Orcus unbeknownst to the legitimate owners of those machines.

The malware researchers noted another reason that Mcgraw couldn't so easily distance himself from how his clients used the software: He and his team are providing ongoing technical support and help to customers who have purchased Orcus and are having trouble figuring out how to infect new machines or hide their activities online.

What's more, the range of features and plugins supported by Armada, they argued, go well beyond what a system administrator would look for in a legitimate remote administration client like Teamviewer, including the ability to launch a keylogger that records the victim's every computer keystroke, as well as a feature that lets the user peek through a victim's Web cam and disable the light on the camera that alerts users when the camera is switched on.

A new feature of Orcus announced July 7 lets users configure the RAT so that it evades digital forensics tools used by malware researchers, including an anti-debugger and an option that prevents the RAT from running inside of a virtual machine.

Other plugins offered directly from Orcus's tech support page (PDF) and authored by the RAT's support team include a "**survey bot**" designed to "make all of your clients do surveys for cash;" a "**USB/.zip/.doc spreader**," intended to help users "spread a file of your choice to all clients via USB/.zip/.doc macros;" a "**Virustotal.com checker**" made to "check a file of your choice to see if it had been scanned on VirusTotal;" and an "**Adsense Injector**," which will "hijack ads on pages and replace them with your Adsense ads and disable adblocker on Chrome."

WHO IS ARMADA?

Gallagher said he was so struck by the guy's "smugness" and sheer chutzpah that he decided to look closer at any clues that Ciriis Mcgraw might have left behind as to his real-world identity and location. Sure enough, he found that Ciriis Mcgraw also has a Youtube account under the same name, and that a video Mcgraw posted in July 2013 pointed to a 33-year-old security guard from Toronto, Canada.

Gallagher noticed that the video — a bystander recording on the scene of a police shooting of a Toronto man — included a link to the domain **policereview[dot]info**. A search of the registration records attached to that Web site name show that the domain was registered to a **John Revesz** in Toronto and to the email address **john.revesz@gmail.com**.

A reverse WHOIS lookup ordered from **Domaintools.com** shows the same john.revesz@gmail.com address was used to register at least 20 other domains, including "thereveszfamily.com," "johnrevesz.com, revesztechnologies[dot]com," and — perhaps most tellingly — "**lordarmada.info**".

Johnrevesz[dot]com is no longer online, but this cached copy of the site from the indispensable **archive.org** includes his personal résumé, which states that John Revesz is a network security administrator whose most recent job in that capacity was as an IT systems administrator for **TD Bank**. Revesz's LinkedIn profile indicates that for the past year at least

he has served as a security guard for **GardaWorld International Protective Services**, a private security firm based in Montreal.

Revesz's CV also says he's the owner of the aforementioned Revesz Technologies, but it's unclear whether that business actually exists; the company's Web site currently redirects visitors to a series of sites promoting spammy and scammy surveys, come-ons and giveaways.

IT'S IN THE EULA, STUPID!

Contacted by KrebsOnSecurity, Revesz seemed surprised that I'd connected the dots, but beyond that did not try to disavow ownership of the Orcus RAT.

"Profit was never the intentional goal, however with the years of professional IT networking experience I have myself, knew that proper correct development and structure to the environment is no free venture either," Revesz wrote in reply to questions about his software. "Utilizing my 15+ years of IT experience I have helped manage Orcus through its development."

Revesz continued:

"As for your legalities question. Orcus Remote Administrator in no ways violates Canadian laws for software development or sale. We neither endorse, allow or authorize any form of misuse of our software. Our EULA [end user license agreement] and TOS [terms of service] is very clear in this matter. Further we openly and candidly work with those prudent to malware removal to remove Orcus from unwanted use, and lock out offending users which may misuse our software, just as any other company would."

Revesz said none of the aforementioned plugins were supported by Orcus, and were all developed by third-party developers, and that "Orcus will never allow implementation of such features, and or plugins would be outright blocked on our part."

In an apparent contradiction to that claim, plugins that allow Orcus users to disable the Webcam light on a computer running the software and one that enables the RAT to be used as a "stresser" to knock sites and individuals users offline are available directly from Orcus Technologies' Github page.

Revesz's also offers a service to help people cover their tracks online. Using his alter ego "Armada" on the hacker forum **Hackforums[dot]net**, Revesz also sells a "bulletproof dynamic DNS service" that promises not to keep records of customer activity.

Dynamic DNS services allow users to have Web sites hosted on servers that frequently change their Internet addresses. This type of service is useful for people who want to host a Web site on a home-based Internet address that may change from time to time, because dynamic DNS services can be used to easily map the domain name to the user's new Internet address whenever it happens to change.

Unfortunately, these dynamic DNS providers are extremely popular in the attacker community, because they allow bad guys to keep their malware and scam sites up even when researchers manage to track the attacking IP address and convince the ISP responsible for that address to disconnect the malefactor. In such cases, dynamic DNS allows the owner of the attacking domain to simply re-route the attack site to another Internet address that he controls.

Free dynamic DNS providers tend to report or block suspicious or outright malicious activity on their networks, and may well share evidence about the activity with law enforcement investigators. In contrast, Armada's dynamic DNS service is managed solely by him, and he promises in his ad on Hackforums that the service — to which he sells subscriptions of various tiers for between $30-$150 per year — will not log customer usage or report anything to law enforcement.

According to writeups by Kaspersky Lab and Heimdal Security, Revesz's dynamic DNS service has been seen used in connection with malicious botnet activity by another RAT known as Adwind. Indeed, Revesz's service appears to involve the domain

“nullroute[dot]pw”, which is one of 21 domains registered to a “Ciriis Mcgraw,” (as well as orcus[dot]pw and orcusrat[dot]pw).

I asked Gallagher (the researcher who originally tipped me off about Revesz’s activities) whether he was persuaded at all by Revesz’s arguments that Orcus was just a tool and that Revesz wasn’t responsible for how it was used.

Gallagher said he and his malware researcher friends had private conversations with Revesz in which he seemed to acknowledge that some aspects of the RAT went too far, and promised to release software updates to remove certain objectionable functionalities. But Gallagher said those promises felt more like the actions of someone trying to cover himself.

“I constantly try to question my assumptions and make sure I’m playing devil’s advocate and not jumping the gun,” Gallagher said. “But I think he’s well aware that what he’s doing is hurting people, it’s just now he knows he’s under the microscope and trying to do and say enough to cover himself if it ever comes down to him being questioned by law enforcement.”