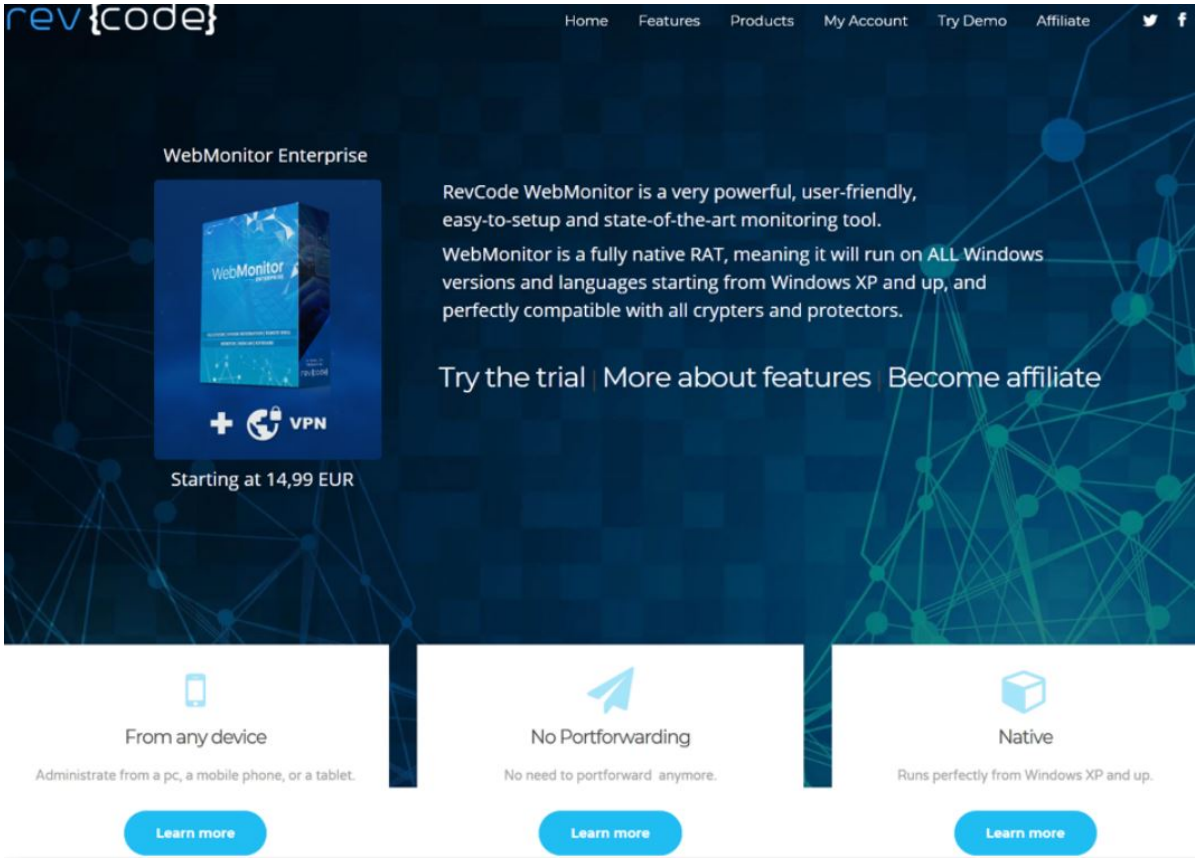
Who's Behind the RevCode WebMonitor RAT?

krebsonsecurity.com/2019/04/whos-behind-the-revcode-webmonitor-rat/

The owner of a Swedish company behind a popular remote administration tool (RAT) implicated in thousands of malware attacks shares the same name as a Swedish man who pleaded guilty in 2015 to co-creating the **Blackshades RAT**, a similar product that was used to infect more than half a million computers with malware, KrebsOnSecurity has learned.



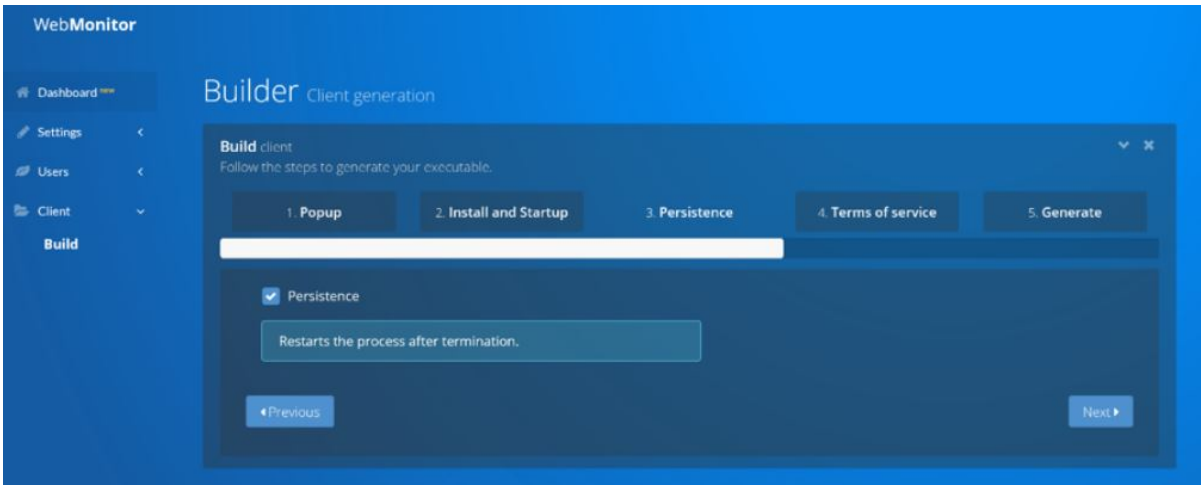
An advertisement for RevCode WebMonitor.

At issue is a program called "**WebMonitor**," which was designed to allow users to remotely control a computer (or multiple machines) via a Web browser. The makers of WebMonitor, a company in Sweden called "**RevCode**," say their product is legal and legitimate software "that helps firms and personal users handle the security of owned devices."

But critics say WebMonitor is far more likely to be deployed on "pwned" devices, or those that are surreptitiously hacked. The software is broadly classified as malware by most antivirus companies, likely thanks to an advertised feature list that includes dumping the remote computer's temporary memory; retrieving passwords from dozens of email programs; snarfing the target's Wi-Fi credentials; and viewing the target's Webcam.

In a writeup on WebMonitor published in April 2018, researchers from security firm **Palo Alto Networks** noted that the product has been primarily advertised on underground hacking forums, and that its developers promoted several qualities of the software likely to appeal to cybercriminals looking to secretly compromise PCs.

For example, RevCode's website touted the software's compatibility with all "crypters," software that can encrypt, obfuscate and manipulate malware to make it harder to detect by antivirus programs. Palo Alto also noted WebMonitor includes the option to suppress any notification boxes that may pop up when the RAT is being installed on a computer.



A screenshot of the WebMonitor builder panel.

RevCode maintains it is a legitimate company officially registered in Sweden that obeys all applicable Swedish laws. A few hours of searching online turned up an interesting record at Ratsit AB, a credit information service based in Sweden. That record indicates RevCode is owned by 28-year-old Swedish resident **Alex Yücel**.

In February 2015, a then 24-year-old Alex Yücel pleaded guilty in a U.S. court to computer hacking and to creating, marketing and selling Blackshades, a RAT that was used to compromise and spy on hundreds of thousands of computers. Arrested in Moldova in 2013 as part of a large-scale, international takedown against Blackshades and hundreds of customers, Yücel became the first person ever to be extradited from Moldova to the United States.

Yücel was sentenced to 57 months in prison, but according to a record for Yücel at the U.S. Federal Bureau of Prisons, he was released on Nov. 1, 2016. The first advertisements in hacker forums for the sale of WebMonitor began in mid-2017. RevCode was registered as an official Swedish company in 2018, according to Ratsit.

Until recently, RevCode published on its Web site a value added tax (VAT) number, an identifier used in many European countries for value added tax purposes. That VAT number — first noted by the blog Krabsonsecurity.com (which borrows heavily from this site's design and banner but otherwise bears no relation to KrebsOnSecurity.com) — has since been

removed from the RevCode Web site and from historic records at The Internet Archive. The VAT number cited in that report is registered to Alex Yücel, and matches the number listed for RevCode by Ratsit AB.

Yücel could not be immediately reached for comment. But an unnamed person responded to an email sent to the customer support address listed at RevCode's site. Presented with the information and links referenced above, the person responding wrote, "nobody working for/with RevCode is in any way related to BlackShades. Anything else suggesting otherwise is nothing but rumors and attempts to degrade our company by means of defamation."

The person responding from the RevCode support email address contended that the Alex Yücel listed as owner of the company was not the same Alex Yücel convicted of co-authoring Blackshades. However, unless the Ratsit record is completely wrong, this seems unlikely to be true.

According to the Ratsit listing, the Alex Yücel who heads RevCode currently lives in a suburb of Stockholm, Sweden with his parents Can and Rita Yücel. Both Can and Rita Yücel co-signed a letter (PDF) in June 2015 testifying to a New York federal court regarding their son's upstanding moral character prior to Yücel the younger's sentencing for the Blackshades conviction, according to court records.

Your Honor,□□

We, Alex Yucel's father and mother, are writing this letter to express our sadness and misery as parents and how sorry we are about this situation regarding Alex.

Alex family and all his relatives and friends are very depressed over this nightmare situation. We all are still very shocked about this incident and the fact that our beloved son Alex is arrested in another country long from Sweden due to a stupide mistake he was not aware of.
We know deep down that Alex is a very kind, good-hearted and honest person, but at the same time he is also extremely naive, which we deeply regret. However, we are absolutely convinced that he has learned a good lesson from this incident and we assure that this will never ever happen again.

We firmly believe that your Honor is fair□and we think that this will shine through in the assessment of Alex case. We hope and pray to God that Alex will come home soon.

Best wishes,

Can Yücel and Rita Yücel

A letter from Alex Yücel's parents to the court in June 2016.