Man jailed for using webcam RAT to spy on women in their bedrooms

tripwire.com/state-of-security/featured/man-jailed-using-webcam-rat-women-bedrooms/

Graham Cluley January 9, 2020

A British man has been jailed for two years after police caught him using a notorious Remote Access Trojan (RAT) to hijack the webcams of young women, and spy upon them.

27-year-old Scott Cowley, of St Helens, Merseyside, was arrested last November as part of an international investigation into purchasers of the Imminent Monitor RAT.

Imminent Monitor (also known as IM-RAT) had been sold online since 2012, purporting to be a legitimate remote access tool.

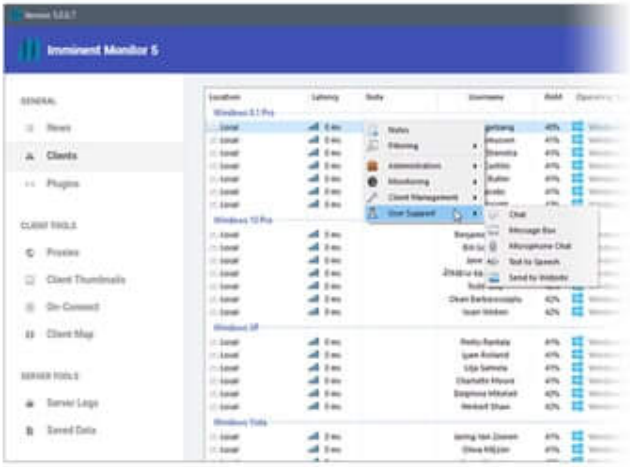
About Imminent Monitor

Imminent Monitor is an advanced System Remote Administration Tool designed for Windows based operating systems, focused on providing a fast, secure and stable replacement for competing products at a significantly lower price.

Imminent Monitor can be used to:

- Fully administer Windows servers remotely
- Provide remote support to clients, friends or colleagues
- Connect to your home computer while you are away
- Monitor employee's work machines
- Connect to your work computer while you are away

Imminent Monitor has been programmed from the ground up by our highly experienced developer with 9+ years of programming experience, over the years Imminent Monitor has received 60+ major free software updates.



Imminent Monitor's claims of legitimacy, however, are somewhat undermined by some of its abilities – such as the ability to allow remote users to disable a subject's webcam light while they are being monitored. One version of the software even introduced the ability to mine for cryptocurrency on victim's PCs.

Security researchers at Palo Alto Networks claim that they have observed Imminent Monitor being used in attacks against its customers on over 115,000 unique occasions.

International law enforcement agencies were finally able to dismantle the infrastructure behind Imminent Monitor last November, in an operation that executed 85 warrants, seized 434 devices, and arrested 13 people.

And, of course, when police cracked the IM-RAT's distribution network they were also able to seize records detailing thousands of purchasers, which resulted in the arrest in Merseyside of Scott Cowley.

At Liverpool Crown Court prosecutors described how the Cowley had used a PayPal account connected to his own name and personal email address to buy the IM-RAT software. Cowley successfully managed to have the software installed on the computers of three women, and seized remote control of their webcams in order to allow him to secretly film them as they undressed and had sex.

Specialist police officers from the North West Regional Organised Crime Unit (NWROCU) were able to forensically examine Cowley's own laptop computer, finding the software as well as furtive video recordings of his victims.

The court found Cowley guilty, and sentenced him to two years imprisonment for computer misuse and sexual offences.

> “Today we welcome the sentencing of Scott Cowley who used highly technological methods to obtain private videos and images of innocent victims for his own sexual gratification. This conviction demonstrates that despite the high tech nature of the Cyber Crime, offenders have no place to hide,” said Detective Sergeant Steve Frame from the NWROCU. “We take all reports of cybercrime seriously and are absolutely committed to tackling and undermining this evolving threat. If you have been the victim of a similar crime, or suspect somebody is involved in committing this type of crime please call 101 and report it to your local police force.”

No doubt police investigations into the users of IM-RAT will continue, and we can hope for more successful prosecutions for those who preyed on innocent computer users.

Editor’s Note: *The opinions expressed in this guest author article are solely those of the contributor, and do not necessarily reflect those of Tripwire, Inc.*