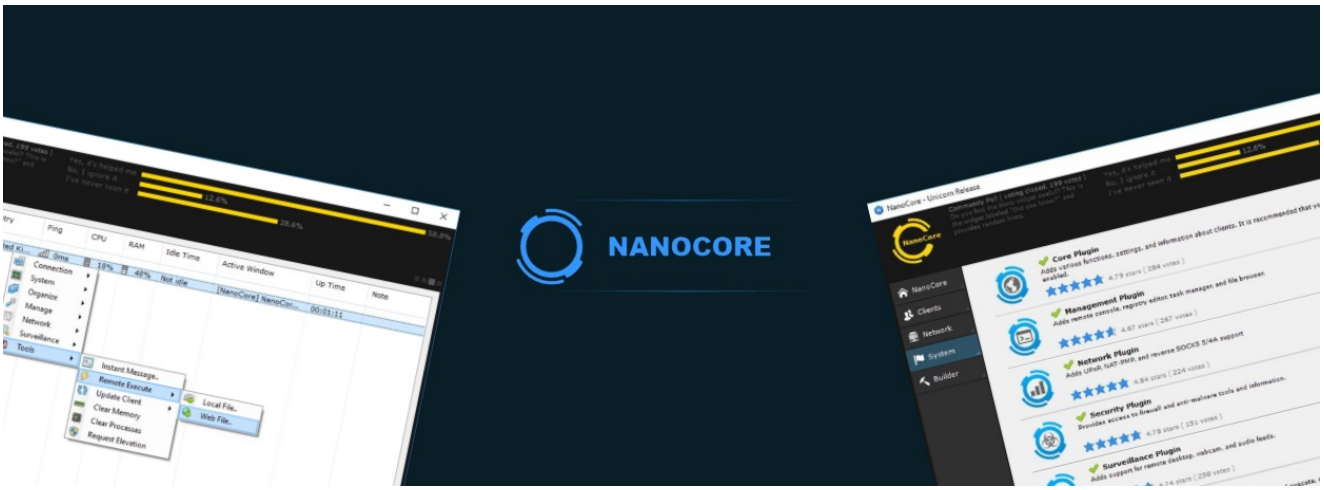
Nanocore RAT Author Gets 33 Months in Prison

bleepingcomputer.com/news/security/nanocore-rat-author-gets-33-months-in-prison/

Catalin Cimpanu

By
Catalin Cimpanu

- February 26, 2018
- 06:07 AM
- 2



US authorities have sentenced an Arkansas man to 33 months in prison and two years of supervised release for aiding and abetting hackers by creating and selling malware.

The man's name is Taylor Huddleston, 27, of Hot Springs, Arkansas. The FBI arrested Huddlestone in early 2017, and Huddleston pleaded guilty in July last year.

Huddleston's case is unique because he was the first case where the author of a malware strain was arrested, despite not being accused of using the malware himself. In the meantime, the US government is pursuing a similar case against Marcus "MalwareTech" Hutchins, the security researcher who helped stop the WannaCry ransomware outbreak, accusing him of creating the Kronos banking trojan.

Huddleston never intended to become a malware author

According to Huddleston's position on sentencing and a statement of facts, the suspect said he did not start out his life as a software engineer with any malicious intent.

Instead, he got into software as a way to sustain himself as a teenager who lived in shabby conditions, never met his biological father, and moved countless of times during his youth.

Huddleston's first major application wasn't even malicious. Called Net Seal, this was a program that could be used to secure applications against software piracy. Net Seal was used with many types of applications, but it became incredibly popular with hackers, who used it to secure malware they put up for sale against scammers and crackers.

Because of his success on the malware scene, and especially Net Seal's popularity on a hacking forum known as HackForums, Huddleston began actively marketing Net Seal on that particular forum in the hopes of boosting revenue.

Huddleston also created the Nanocore RAT

But as his ties to the cybercrime world deepened, so did his morals. Two years after starting to advertise Net Seal on HackForums, Huddleston created Nanocore, which he described and advertised on the same forum as a "remote access tool ... designed to allow a computer hacker to take complete control of a victim's computer for the purpose of performing" remote operations.

Huddleston advertised and sold the Nanocore RAT on HackForums under the nickname of Aeonhack from January 2014 to February 2016, when he sold both Net Seal and Nanocore to an unidentified third-party.

In his guilty plea, Huddleston admitted to knowing that some of his customers used Nanocore for malicious purposes. Before pleading guilty, Huddleston's lawyer tried to argue that in many of reported Nanocore infections [1, 2, 3], Huddleston wasn't even aware of the attacks and that some malware distributors used cracked versions of his RAT.

Mr. Huddleston understands and accepts that he broke the law by marketing Net Seal and NanoCore on a website frequented by users who would likely use the programs for malicious purposes. [...] Mr. Huddleston knows that he has no one to blame but himself, and is prepared to serve the sentence this Court finds appropriate. His actions before and after his arrest illustrate his sincere remorse and dedication to using his talents to benefit society and make amends for his illegal conduct.

Huddleston now works as a carpenter, his lawyers told the court before last week's sentencing. He also "enthusiastically" cooperated with authorities, his lawyers pointed out.

They asked for a maximum sentence of six months in prison. He faced a maximum prison sentence of ten years, but the court decided on 33 months instead.

The FBI tracked down Huddleston during their investigation of Zachary Shames, the author of the Limitless Keylogger.

Related Articles:

New stealthy Nerbian RAT malware spotted in ongoing attacks

New NetDooka malware spreads via poisoned search results

New ChromeLoader malware surge threatens browsers worldwide

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps

Popular Python and PHP libraries hijacked to steal AWS keys

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.