MUST READ: Resetting the 5G goalposts: How the US declares victory

FBI arrests alleged NullCrew hacktivist

The FBI has arrested an alleged member of the NullCrew hacktivist group following cyberattacks on businesses and universities.

By Charlie Osborne for Zero Day | June 19, 2014 -- 09:47 GMT (02:47 PDT) | Topic: Security

The US Department of Justice has charged a man who allegedly participated in high-profile cyberattacks against corporations, universities and government agencies.

In a statement released Wednesday (http://www.justice.gov/usao/iln/pr/chicago/2014/pr0616_01.html), the DoJ said Timothy French, 20, was arrested in Tennessee last week and is being charged with "federal computer hacking for allegedly conspiring to launch cyber attacks on two universities and three companies" as part of the hacktivist collective called NullCrew.

Through these attacks, thousands of account names and passwords were stolen and published online.

While the DoJ has not released the names of the companies, universities and governmental bodies that were targeted, the agency said that in one case, a successful cyberattack launched by NullCrew resulted in over 3,000 usernames, email addresses and passwords belonging to a foreign government's ministry of defense to be released on the web. According to NullCrew's claims in 2012, the United Kingdom was the target.

The law enforcement agency says social media sites and Skype are frequent tools used by NullCrew to select targets, organize cyberattacks and declare successful campaigns. Twitter, for example, is often used to link to PasteBin files containing data dumps — information acquired after breaching a target's security.

If found guilty of his role in NullCrew hacktivist campaigns, French faces up to 10 years in prison and a fine of up to $250,000.

In a statement, United States Attorney for the Northern District of Illinois Zachary T. Fardon said:

> Cybercrime sometimes involves new-age technology but age-old criminal activity — unlawful intrusion, theft of confidential information, and financial harm to victims. Hackers who think they can anonymously steal private business and personal information from computer systems should be aware that we are determined to find them, to prosecute pernicious online activity, and to protect cybervictims.

VR AND AR

Microsoft's HoloLens 2 looks ready to go on sale in September (https://www.zdnet.com/article/microsofts-hololens-2-looks-ready-to-go-on-sale-in-september/)

Meltdown averted: How VR headsets are making nuclear power plants safer (https://www.zdnet.com/article/meltdown-averted-how-virtual-worlds-are-making-nuclear-power-plants-safer/)

Space robots remotely controlled in VR (https://www.zdnet.com/article/space-robots-remotely-controlled-through-vr/)

Using AR and VR to train surgeons (ZDNet YouTube) (https://www.youtube.com/watch?v=lFpSw8lY4mA)

Best VR headsets for 2019 (CNET) (https://www.cnet.com/news/best-vr-headsets-for-2019/?ftag=CMG-01-10aaa1b)

Virtual reality: A cheat sheet for business pros (TechRepublic) (https://www.techrepublic.com/article/virtual-reality-a-cheat-sheet-for-business-pros/?ftag=CMG-01-10aaa1b)

Following the arrest, a member of NullCrew released a statement on PasteBin (http://pastebin.com/hWhzkmGg) taunting French and lamenting the presence of "skids" — script kiddies — within the group. A reference is also made to the case of Sabu, who turned informer as part of the LulzSec hacking crew. Despite facing up to 26 years behind bars for his role in cyberattacks against high-profile targets — including Sony (/article/second-accused-lulzsec-hacker-arrested-in-us/) , Nintendo and news outlets — his cooperation with the FBI allowed him to walk free from jail (/article/snitch-lulzsec-hacker-sabu-walks-free-after-assisting-fbi/) .

"Don't let just any asshole in the crew, and don't give them the keys to the fucking kingdom," the member said. "The FBI got someone to get you fuckers, and you deserved it. I've already taken care of that little problem — if it walks like Sabu and talks like Sabu..."

The NullCrew statement also described how law enforcement agencies may have tracked down the alleged member, as well as one more member who has not been confirmed by the FBI:

> I told that fucking idiot Timmy (c0rps3, Orb1t_G1rl, rootcrysis) that his dox was too easy to find and provided ways for him to escape it. He obviously didn't. And Dominik (thebinkyp, zer0pwn, phlex, nop_nc, docofcocks, theindigator, NULL), you seemed to think that no one would ever find your old aliases? Maybe you've never seen the hackforums dump that showed thebinkyp = zer0pwn? Maybe you deserved to get fucking burned for being on hackforums in the first place?
>
> Next, your OpSec was fucking horrendous. Don't launch attacks from your home IPs, skidlets! Don't log into our compromised servers from your home IPs! Fucking get a clue, get a fucking VPN! Doxxing these two morons was super simple, which explains why the FBI could do it. Did you really think they wouldn't subpoena Skype, fucking told you Timmy.

RELATED TOPICS: SECURITY TV DATA MANAGEMENT CXO DATA CENTERS

By Charlie Osborne for Zero Day | June 19, 2014 -- 09:47 GMT (02:47 PDT) | Topic: Security

SHOW COMMENTS