How BreachForums' 'Pompompurin' Led the FBI to His Home

Police: Fitzpatrick Waived Right to Silence, Confessed to Starting & Running Forum

BY David Perera (@daveperera) • March 24, 2023 (link)

The alleged administrator of criminal online forum BreachForums may have thought he took steps to hide his real identity, but instead he left a trail of digital breadcrumbs that led to his arrest and prosecution, shows information unsealed in federal court.

Federal agents questioned Conor Brian Fitzpatrick, 20, raiding his parent's Peekskill, New York house in the early hours of March 15 after concluding that he was "Pompompurin," owner of BreachForums. Police say Fitzpatrick waived his right to silence and confessed to launching and maintaining the forum used by cybercriminals to sell stolen data. Fitzpatrick told law enforcement he earned approximately $1,000 a day from BreachForums, mainly through members who paid for credits to access hacked data and for membership upgrades on the now-offline site (see: *BreachForums Closes Amid Worries Over Law Enforcement Access*).

"BreachForums bridged the gap between hackers hawking pilfered data and buyers eager to exploit it. All those operating in darknet markets should take note: Working with our law enforcement partners, we will take down illicit forums and bring administrators to justice in U.S. courtrooms," said Deputy Attorney General Lisa O. Monaco in a statement Friday following Fitzpatrick's first appearance in a federal court.

An FBI affidavit unsealed in federal court Thursday shows that feds began the hunt for Pompompurin with a list of IP addresses he allegedly used to connect to BreachForums' dismantled predecessor, RaidForums. Pompompurin was an active member of RaidForums until its February 2022 demise at the hands of law enforcement and communicated with its administrator, allegedly Portuguese national Diogo Santos Coelho, who went by the online handle "omnipotent." Authorities arrested Coelho in the United Kingdom in January 2022.

Records obtained from telecom provider Verizon showed that some of the IP addresses the RaidForums user Pompompurin used to connect to RaidForums were associated with a mobile device registered to Conor Fitzpatrick at his parents' Hudson Valley address.

Prosecutors say Fitzpatrick did take pains to hide his real IP address by using multiple VPNs. "These services are occasionally misconfigured and expose the user's true IP address," wrote FBI agent John Longmire in the affidavit.

Agents also found communication showing that Pompompurin mentioned searching a breached database with an old email address: conorfitzpatrick02@gmail.com. Knowledge of that email led agents to find the active email address conorfitzpatrick2002@gmail.com and obtain information from Google showing that both Gmail addresses were registered under the name "Conor Fitzpatrick" and associated with his Peekskill address and Verizon cell number.

IP and email address matching among online service providers, including Zoom and online cryptocurrency e-shopping site Purse.io, also pointed back to Fitzpatrick. By October 2022, the FBI had zeroed in on him to the point where it obtained a cellphone GPS warrant on his Verizon phone and matched activity of the BreachForums Pompompurin account to within 1 kilometer of his Peekskill home. Agents also began actively surveilling the house, observing activity on the Pompompurin account while Fitzpatrick was at home.

Prosecutors say more than 14 billion leaked records were available on BreachForums. Among them were the names and contact information for approximately 200 million Twitter users. Another user posted data stolen earlier this month from the online health insurance marketplace used by members of Congress and residents of Washington, D.C.

A BreachForums user in December also posted details of approximately 87,760 members of InfraGard, a partnership between the FBI and private sector companies focused on the protection of critical infrastructure (see: *Hacker Reportedly Breaches US FBI Cybersecurity Forum*).