



## Who's Behind the Seized Forums 'Cracked' & 'Nulled'?

February 4, 2025

16 Comments

The **FBI** joined authorities across Europe last week in seizing domain names for **Cracked** and **Nulled**, English-language cybercrime forums with millions of users that trafficked in stolen data, hacking tools and malware. An investigation into the history of these communities shows their apparent co-founders quite openly operate an Internet service provider and a pair of e-commerce platforms catering to buyers and sellers on both forums.

In this 2019 post from Cracked, a forum moderator told the author of the post (Buddie) that the owner of the RDP service was the founder of Nulled, a.k.a. "Finndev." Image: Ke-la.com.

On Jan. 30, the **U.S. Department of Justice** said it seized eight domain names that were used to operate Cracked, a cybercrime forum that sprang up in 2018 and attracted more than four million users. The DOJ said the law enforcement action, dubbed **Operation Talent**, also seized domains tied to **Sellix**, Cracked's payment processor.

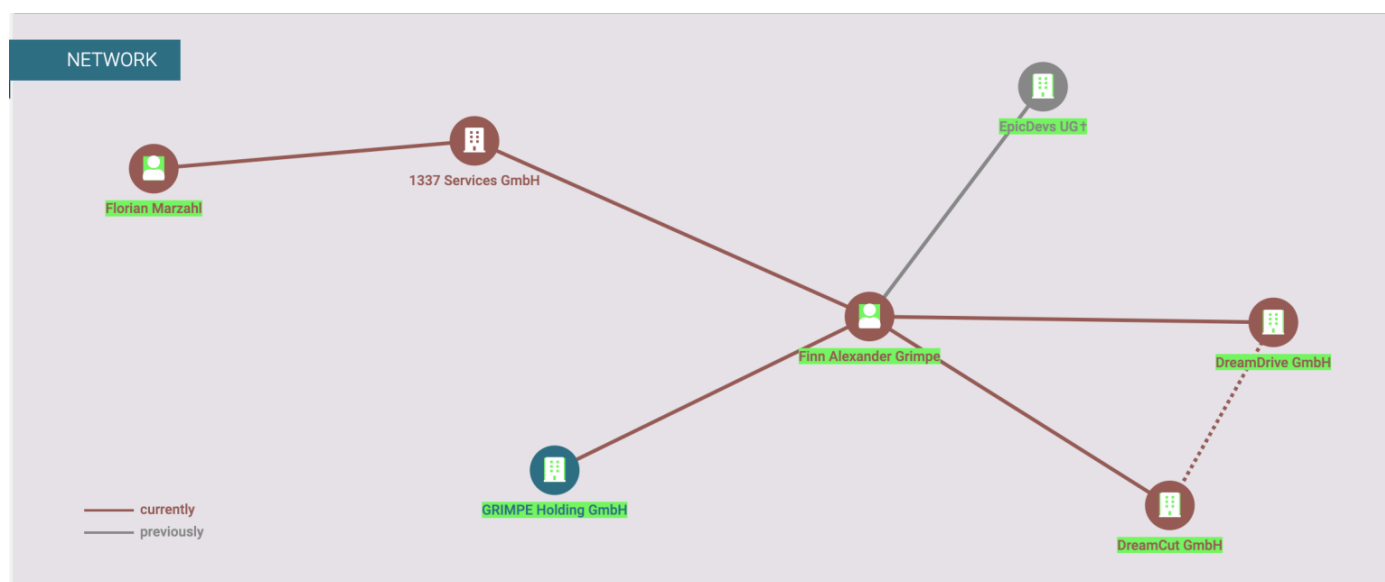
In addition, the government seized the domain names for two popular anonymity services that were heavily advertised on Cracked and Nulled and allowed customers to rent virtual servers:

[StarkRDP\[.\]io](#), and [rdp\[.\]sh](#).

Those archived webpages show both RDP services were owned by an entity called **1337 Services GmbH**. According to [corporate records](#) compiled by **Northdata.com**, 1337 Services GmbH is also known as **AS210558** and is incorporated in Hamburg, Germany.

The Cracked forum administrator went by the nicknames “**FlorainN**” and “**StarkRDP**” on multiple cybercrime forums. Meanwhile, a [LinkedIn profile](#) for a **Florian M.** from Germany refers to this person as the co-founder of Sellix and founder of 1337 Services GmbH.

Northdata's business profile for 1337 Services GmbH shows the company is controlled by two individuals: 32-year-old **Florian Marzahl** and **Finn Alexander Grimpe**, 28.



An organization chart showing the owners of 1337 Services GmbH as Florian Marzahl and Finn Grimpe. Image: Northdata.com.

Neither Marzahl nor Grimpe responded to requests for comment. But Grimpe's first name is interesting because it corresponds to the nickname chosen by the founder of Nulled, who goes by the monikers “**Finn**” and “**Finndev**.” NorthData reveals that Grimpe was the founder of a German entity called **DreamDrive GmbH**, which rented out [high-end sports cars and motorcycles](#).

According to the cyber intelligence firm [Intel 471](#), a user named Finndev registered on multiple cybercrime forums, including **Raidforums** [\[seized by the FBI in 2022\]](#), **Void[.]to**, and **vDOS**, a DDoS-for-hire service that was [shut down in 2016 after its founders were arrested](#).

The email address used for those accounts was **f.grimpe@gmail.com**. [DomainTools.com](#) reports **f.grimpe@gmail.com** was used to register at least nine domain names, including **nulled[.]lol** and **nulled[.]it**. Neither of these domains were among those seized in Operation Talent.

Intel471 finds the user FlorainN registered across multiple cybercrime forums using the email address **olivia.messla@outlook.de**. The breach tracking service [Constella Intelligence](#) says this email address used the same password (and slight variations of it) across many accounts online

— including at hacker forums — and that the same password was used in connection with dozens of other email addresses, such as **florianmarzahl@hotmail.de**, and **fmarzahl137@gmail.com**.

The Justice Department said the Nulled marketplace had more than five million members, and has been selling stolen login credentials, stolen identification documents and hacking services, as well as tools for carrying out cybercrime and fraud, since 2016.

Perhaps fittingly, both Cracked and Nulled have been hacked over the years, exposing countless private messages between forum users. A review of those messages archived by Intel 471 showed that dozens of early forum members referred privately to Finndev as the owner of **shoppy[.]gg**, an e-commerce platform that caters to the same clientele as Sellix.

Shoppy was not targeted as part of Operation Talent, and its website remains online. Northdata **reports** that Shoppy's business name — **Shoppy Ecommerce Ltd.** — is registered at an address in Gan-Ner, Israel, but there is no ownership information about this entity. Shoppy did not respond to requests for comment.

Constella found that a user named Shoppy registered on Cracked in 2019 using the email address **finn@shoppy[.]gg**. Constella says that email address is tied to **a Twitter/X account** for Shoppy Ecommerce in Israel.

The DOJ said one of the alleged administrators of Nulled, a 29-year-old Argentinian national named **Lucas Sohn**, was arrested in Spain. The government has not announced any other arrests or charges associated with Operation Talent.

Indeed, both StarkRDP and FloraiN have posted to their accounts on **Telegram** that there were no charges levied against the proprietors of 1337 Services GmbH. FlorainN told former customers they were in the process of moving to a new name and domain for StarkRDP, where existing accounts and balances would be transferred.

"StarkRDP has always been operating by the law and is not involved in any of these alleged crimes and the legal process will confirm this," the StarkRDP Telegram account wrote on January 30. "All of your servers are safe and they have not been collected in this operation. The only things that were seized is the website server and our domain. Unfortunately, no one can tell who took it and with whom we can talk about it. Therefore, we will restart operation soon, under a different name, to close the chapter [of] 'StarkRDP.'"

*This entry was posted on Tuesday 4th of February 2025 12:09 PM*

A LITTLE SUNSHINE

BREADCRUMBS

1337 SERVICES GMBH AS210558 CONSTELLA INTELLIGENCE CRACKED DOMAINTOOLS

DREAMDRIVE GMBH FINN ALEXANDER GRIMPE FINN@SHOPPY.GG FINNDEV FLORIAN FLORIAN

MARZAHN HRB 164175 INTEL 471 LUCAS SOHN NORTHDATA.COM NULLED