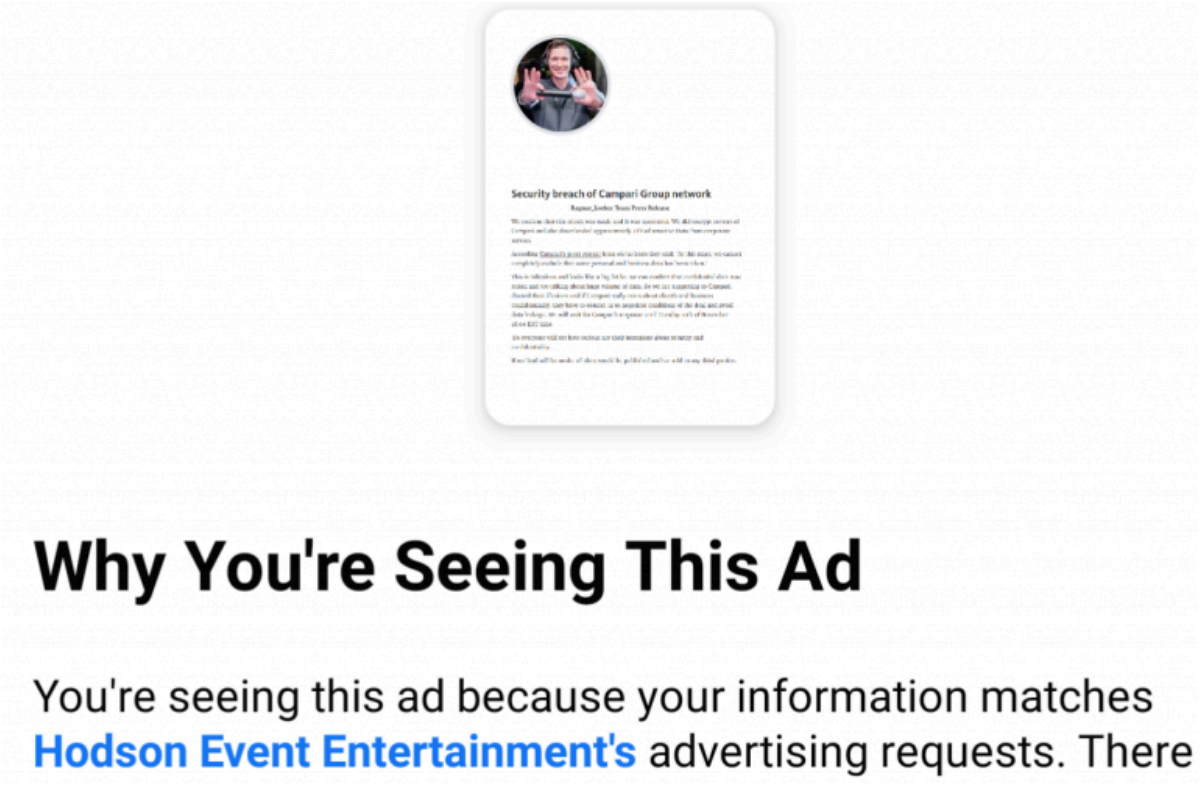
Ransomware Group Turns to Facebook Ads

Published: 2020-11-10 · Archived: 2026-04-05 15:33:42 UTC

It's bad enough that many ransomware gangs now have blogs where they publish data stolen from companies that refuse to make an extortion payment. Now, one crime group has started using hacked **Facebook** accounts to run ads publicly pressuring their ransomware victims into paying up.



On the evening of Monday, Nov. 9, an ad campaign apparently taken out by the Ragnar Locker Team began appearing on Facebook. The ad was designed to turn the screws to the Italian beverage vendor **Campari Group**, which acknowledged on Nov. 3 that its computer systems had been sidelined by a malware attack.

On Nov. 6, Campari issued a follow-up statement saying "at this stage, we cannot completely exclude that some personal and business data has been taken."

"This is ridiculous and looks like a big fat lie," reads the Facebook ad campaign from the Ragnar crime group. "We can confirm that confidential data was stolen and we talking about huge volume of data."

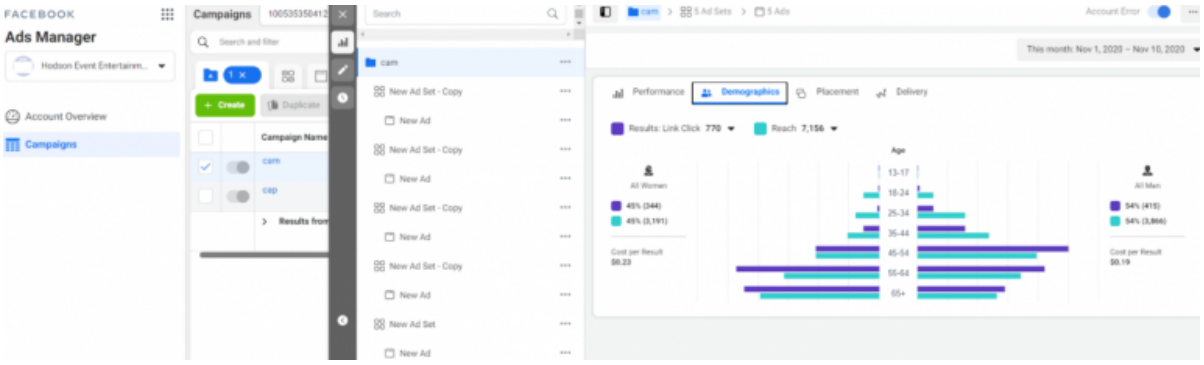
The ad went on to say Ragnar Locker Team had offloaded two terabytes of information and would give the Italian firm until 6 p.m. EST today (Nov. 10) to negotiate an extortion payment in exchange for a promise not to publish the stolen files.

The Facebook ad blitz was paid for by **Hodson Event Entertainment**, an account tied to Chris Hodson, a deejay based in Chicago. Contacted by KrebsOnSecurity, Hodson said his Facebook account indeed was hacked, and that

the attackers had budgeted $500 for the entire campaign.

“I thought I had two-step verification turned on for all my accounts, but now it looks like the only one I didn’t have it set for was Facebook,” Hodson said.

Hodson said a review of his account shows the unauthorized campaign reached approximately 7,150 Facebook users, and generated 770 clicks, with a cost-per-result of 21 cents. Of course, it didn’t cost the ransomware group anything. Hodson said Facebook billed him $35 for the first part of the campaign, but apparently detected the ads as fraudulent sometime this morning before his account could be billed another $159 for the campaign.



The results of the unauthorized Facebook ad campaign. Image: Chris Hodson.

It’s not clear whether this was an isolated incident, or whether the fraudsters also ran ads using other hacked Facebook accounts. A spokesperson for Facebook said the company is still investigating the incident. A request for comment sent via email to Campari’s media relations team was returned as undeliverable.

But it seems likely we will continue to see more of this and other mainstream advertising efforts by ransomware groups going forward, even if victims really have no expectation that paying an extortion demand will result in criminals actually deleting or not otherwise using stolen data.

Fabian Wosar, chief technology officer at computer security firm Emsisoft, said some ransomware groups have become especially aggressive of late in pressuring their victims to pay up.

“They have also started to call victims,” Wosar said. “They’re outsourcing to Indian call centers, who call victims asking when they are going to pay or have their data leaked.”

Source: https://krebsonsecurity.com/2020/11/ransomware-group-turns-to-facebook-ads/