Data From The Emotet Malware is Now Searchable in Have I Been Pwned, Courtesy of the FBI and NHTCU

By Troy Hunt

Published: 2021-04-26 · Archived: 2026-04-05 22:26:16 UTC

Earlier this year, the FBI in partnership with the Dutch National High Technical Crimes Unit (NHTCU), German Federal Criminal Police Office (BKA) and other international law enforcement agencies brought down what Europol rereferred to as the world's most dangerous malware: Emotet. This strain of malware dates back as far as 2014 and it became a gateway into infected machines for other strains of malware ranging from banking trojans to credential stealers to ransomware. Emotet was extremely destructive and wreaked havoc across the globe before eventually being brought to a halt in February.

Following the takedown, the FBI reached out and asked if Have I Been Pwned (HIBP) might be a viable means of alerting impacted individuals and companies that their accounts had been affected by Emotet. This isn't the first time HIBP has been used by law enforcement in the wake of criminal activity with the Estonian Central Police using it for similar purposes a few years earlier.

In all, 4,324,770 email addresses were provided which span a wide range of countries and domains. The addresses are actually sourced from 2 separate corpuses of data obtained by the agencies during the takedown:

1. Email credentials stored by Emotet for sending spam via victims' mail providers
2. Web credentials harvested from browsers that stored them to expedite subsequent logins

We discussed loading these into HIBP as 2 separate incidents so they could be individually identified, but given the remediation is very similar they've been loaded in as a single "breach". Prepared in conjunction with the FBI, following is the recommended guidance for those that find themselves in this collection of data:

1. Keep security software such as antivirus up to date with current definitions. I personally use Microsoft Defender which is free, built into Windows 10 and updates automatically via Windows Update.
2. Change your email account password. Also change passwords and security questions for any accounts you may have stored in either your inbox or browser, especially those of higher value such as banking.
3. For administrators with affected users, refer to the YARA rules released by DFN Cert, which include rules published by the German BKA.

In addition, all the old security best practices are obviously still important whether you find yourself in this incident or not: Use a password manager and create strong, unique passwords. Turn on 2 factor authentication wherever available. Keep operating systems and software patched.

I've flagged this incident as sensitive in HIBP which means it's not publicly searchable, rather individuals will either need to verify control of the address via the notification service or perform a domain search to see if they're

impacted. I've taken this approach to avoid anyone being targeted as a result of their inclusion in Emotet. All impacted HIBP subscribers have been sent notifications already.

Have I Been Pwned
Tweet Post Update Email RSS

Troy Hunt

Hi, I'm Troy Hunt, I write this blog, create courses for Pluralsight and am a Microsoft Regional Director and MVP who travels the world speaking at events and training technology professionals

---

Source: https://www.troyhunt.com/data-from-the-emotet-malware-is-now-searchable-in-have-i-been-pwned-courtesy-of-the-fbi-and-nhtcu/