# What is Pastebin and Why Do Hackers Love It?

By Alex Ciarniello

Archived: 2026-04-05 19:40:51 UTC

Alex Ciarniello September 24, 2019

Pastebin is a website that allows users to share plain text through public posts called “pastes.” The site currently has 17 million unique monthly users. Why is it so popular, and where did it come from?

There are many similar web applications, known as “paste sites,” that have developed since the original Pastebin was launched in 2002. The need for Pastebin rose out of user activity on the Internet Relay Chat (IRC). IRC is an instant messaging application launched in 1988. It’s designed for a large user base to communicate in real-time, and is popular for sharing plain text, including blocks of source code.



Codesharing directly in IRC channels (and other messaging applications) disrupts the flow of messages or can alter the code itself. Users require a third-party site where they can share plain text blocks as a link, allowing other users to easily access and edit it. Enter: paste sites.

While paste sites mainly support innocuous text-sharing, they have also become popular platforms for illegal activities, such as leaking breached data.

## What do people share on Pastebin and other paste sites?


sharing source code on pastebin sites

Paste sites are commonly used for sharing code. However, any data in text form can be uploaded and shared. Users can use the Pastebin search tool to find relevant content based on keyword. The following are some common paste site uses:

- As an alternative to sharing text files in applications like Google Docs
- Twitter users sharing updates longer than the 140 character limit often tweet a paste link with the complete text
- Uploading source code for the purpose of sharing or review/collaboration

- Spam/site promotion
- Re-publishing text that has been removed from other sites
- Sharing dark web links
- Publicizing breached data and other sensitive information



## How do adversaries use paste sites?

As it might be clear from the list above, paste sites are often used for nefarious purposes. In fact, Pastebin was sold to its current owner Jeroen Vader in 2009 after the site was shut down due to a Hotmail data breach.

Pastebin's FAQ page currently prohibits posting:

- Email addresses and password lists
- Login details
- Stolen source code
- Hacked data
- Copyrighted information
- Banking, credit card, or financial information
- Personal information
- Pornographic information
- Spam links, including site promotion

These items are examples of how paste sites are used by adverse hackers. Pastebin specifically is user-friendly, supports large text files, doesn't require user registration, and allows for anonymous posting if the user has a VPN. It also relies on users for reporting abuses, which means non-compliant pastes are not always flagged or removed immediately. This allows black hat hackers to easily and anonymously breach data in an accessible place.

Pastebin and similar sites are hosted on the deep web. This means that they're viewable in a regular internet browser, but the content is not indexed by Google and other conventional search engines. Users must use the site's internal keyword search tool to find specific content, or get paste links directly from other users.

There are also paste sites on the dark web that offer heightened anonymity through a Tor browser, catering exclusively to illegal activity. For example, the dark web's DeepPaste is primarily used for advertising illegal goods or services (e.g. financial fraud, ransomware, child pornography, human trafficking, narcotics), and personally identifiable information breaches (doxxing). Site admins are prohibited from censoring or deleting content, which means that pretty much anything goes.

## What has been leaked on paste sites?

 credit card information shared on pastebin sites

Here are a few headline-worthy leaks discovered on Pastebin and DeepPaste.

### Sony Pictures

In October 2014, Sony Pictures' computer systems were hacked by a group known as Guardians of Peace (GOP). The hack breached a large amount of data to Pastebin, including employee information for over a million individuals, upcoming production details, and music codes. Pastebin was inundated with traffic as links to this information were uploaded.

### Infragard

Another hacker group known as LulzSec leaked the user base of Infragard, an FBI affiliate based in Atlanta, on Pastebin. 180 of Infragard's logins were exposed, as well as email communications that revealed sensitive intel about a U.S. operation to control Libyan cyberspace.

### Google vs. Facebook

Pastebin's highest ever traffic volume occurred in May 2011 after a user posted email correspondence between a Facebook-backed PR agency and Chris Soghoian, an internet security blogger. In the emails, the agency declined to disclose their client (Facebook), and pitched an anti-Google op-ed piece questioning Google's user privacy standards.

### Ring

In December 2019, Amazon Ring customers were compromised in a public breach posted to DeepPaste. The breach leaked data for over 3,000 sold cameras, including the customer emails and passwords. This data enabled hackers to access customer addresses, camera footage, and financial data.



## Paste sites and Beacon


Paste sites are valuable data sources for cybersecurity teams and public safety officials seeking threat intelligence. Information linked to security breaches, doxxing or personal information leaks, hacked financial data, stolen source code, and other criminal activity is all useful for investigating cyber crimes and mitigating threats.

Given that pastes sites are hosted on the deep and dark web, finding relevant content is cumbersome and potentially dangerous without specialized search tools. Pastes might also be taken down by moderated sites before you are able to find their links.

These challenges necessitate tools that can search for relevant data on unindexed websites like Pastebin and dark websites like DeepPaste. Echosec Systems dark web tool, Beacon, also indexes deep websites like Pastebin. Users can search unindexed content on the deep and dark web by keyword and other search filters, and separate data specifically crawled from paste site sources. Relevant pastes are easier and faster to find—and if they've been removed by moderators, the content is still viewable within Beacon, as long as retaining that paste is in compliance with Pastebin's terms of use.

In addition to data discovery tools like Beacon, Echosec Systems also offers a proprietary Platform API, which uses AI classifiers to find data breaches and toxicity on Pastebin and DeepPaste. The API gives Beacon users broader data access to these sources than other commercial APIs. It can also be used independently as a raw data source to support organizations with existing threat intelligence tools.

The dark web isn't the only place with relevant intel for threat detection. Open websites like Pastebin have become popular sites for hackers to breach sensitive information. Being able to quickly and easily access this information requires advanced threat discovery tools.

Book a demo today and see how Beacon can streamline your cyber investigations process.

**BOOK A DEMO**

---