





**Matthew on X: "  #BruteRatel: Static detection via API hashes  
Very similar to the Havoc C2 Detector. Looks for API hashes used  
to resolve ntdll functions. 8/8 Files successfully detected (on disk) 1/  
   <https://t.co/kZYvPJ3UAc> #Ghidra #Malware #Yara  
<https://t.co/6LHzCpIGvI>" / X**

Published: 2022-10-12 · Archived: 2026-04-05 13:14:02 UTC

Did someone say ... cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly.

---

Source: [https://twitter.com/embee\\_research/status/1580030303950995456?s=20&t=0vfXnrCXaVsx-P-hiSrFwA](https://twitter.com/embee_research/status/1580030303950995456?s=20&t=0vfXnrCXaVsx-P-hiSrFwA)