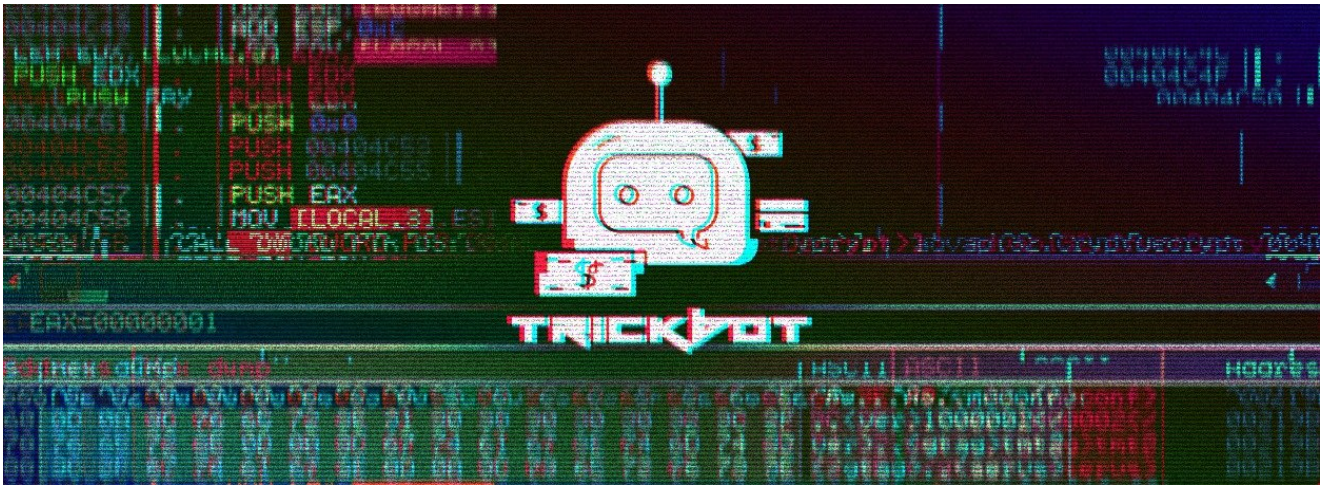
TrickBot malware mistakenly warns victims that they are infected

bleepingcomputer.com/news/security/trickbot-malware-mistakenly-warns-victims-that-they-are-infected/

Lawrence Abrams

By
Lawrence Abrams

- July 11, 2020
- 02:12 PM
- 0



The notorious TrickBot malware mistakenly left a test module that is warning victims that they are infected and should contact their administrator.

TrickBot is a malware infection that is commonly distributed via malicious spam emails. When installed, the malware will run quietly on a victim's machine while it downloads various modules that perform different tasks on the infected computer.

These modules allow the malware to steal a domain's Active Directory Services database, harvest browser passwords and cookies, steal OpenSSH keys, and spread laterally throughout a network.

To make matters worse, TrickBot is known to finalize their attacks by giving access to ransomware operators such as Ryuk and Conti.

TrickBot devs made a mistake

In a recent release of the TrickBot malware analyzed by Advanced Intel's Vitali Kremez, the threat actors are mistakenly distributing a test version of their password-stealing grabber.dll module.

When loaded, this module displays a warning in the default browser stating that the program is gathering information and that the victim should ask their system administrator.

The warning shown by TrickBot's grabber module

```
Warning
You see this message because the program named grabber gathered some information from
your browser.
If you do not know what is happening it is the time to start be worrying.
Please, ask your system administrator for details.
```

This warning is not an isolated case either as BleepingComputer found a user infected with TrickBot who posted about this warning 16 days ago on Reddit.

"Firefox is warning me about a "program named grabber." What is it and what should I do?," the Reddit user asked.

Grabber.dll is TrickBot's password and cookie-stealing module that attempts to harvest saved browser credentials and cookies from Chrome, Edge, Internet Explorer, and Firefox. These stolen credentials and cookies can then be used to login to the victim's accounts.

Kremez was able to extract the documentation embedded in the module, which we shared below.

```
Gathers info from local installed browsers and saves it to files.
Default saving directory is ./confs (executable path subdir)
Browser selection:
  -a, --all[[=]flags]               All known browsers (default)
  -F, --firefox[[=][flags],FILE]    Mozilla Firefox browser (registry search)
  -C, --chrome[[=][flags],FILE]     Google Chrome (registry search)
  -E, --edge[[=][flags],FILE]       Microsoft Edge (supposing Windows 10 and later
has only)
  -I, --iexplorer[[=][flags],FILE]  Microsoft Internet Explorer
Miscellaneous:
  -L, --lso[=][,]FILE               Save common flash lso files (browser independent,
lso managment)
  -s, --silent                      Display only critical errors
  -v, --verbose                     Increase verbosity level
  -V, --version                     Display version information and exit
  -h, --help                        Display this help text and exit
```

For a detailed technical analysis of this grabber.dll module, Kremez published a blog post on the Advanced Intel site.

Kremez told BleepingComputer that the test module appears to be developed by the TrickBot devs as it is "coded in the same fashion" as other modules. He believes that the threat actors were testing a new version and forgot to remove it when it went live.

For those seeing this warning, Kremez advises that victims immediately disconnect their computer from the network and then perform a scan with their installed security software.

Once your computer has been cleaned, victims should change their passwords at any site, external or internal, whose credentials are saved in the browser or recently logged into from the browser.

If a victim is on a corporate network, other computers may have also been compromised, and a thorough investigation should be undertaken.

Related Articles:

Ukraine warns of “chemical attack” phishing pushing stealer malware

Pixiv, DeviantArt artists hit by NFT job offers pushing malware

Google exposes tactics of a Conti ransomware access broker

New powerful Prynt Stealer malware sells for just $100 per month

New ZingoStealer infostealer drops more malware, cryptominers

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence

Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.