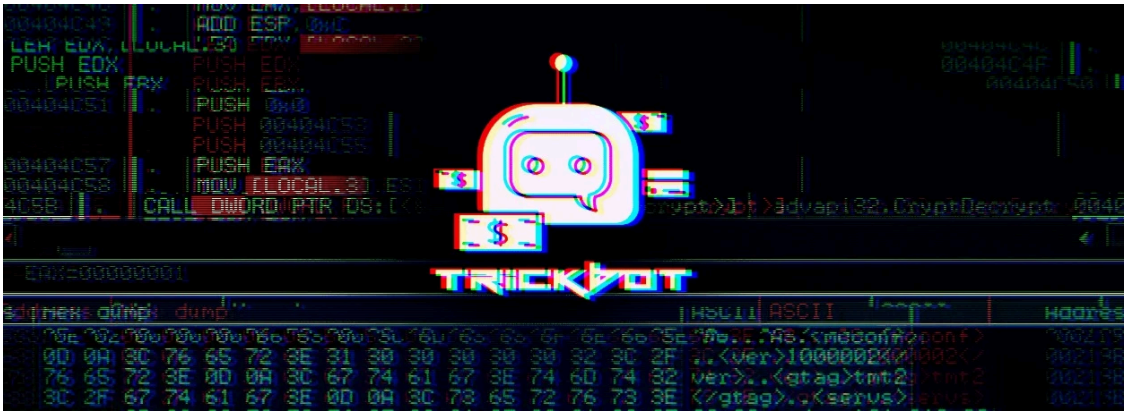
TrickBot malware now checks screen resolution to evade analysis

By Lawrence Abrams

Published: 2020-07-01 · Archived: 2026-04-05 13:46:51 UTC

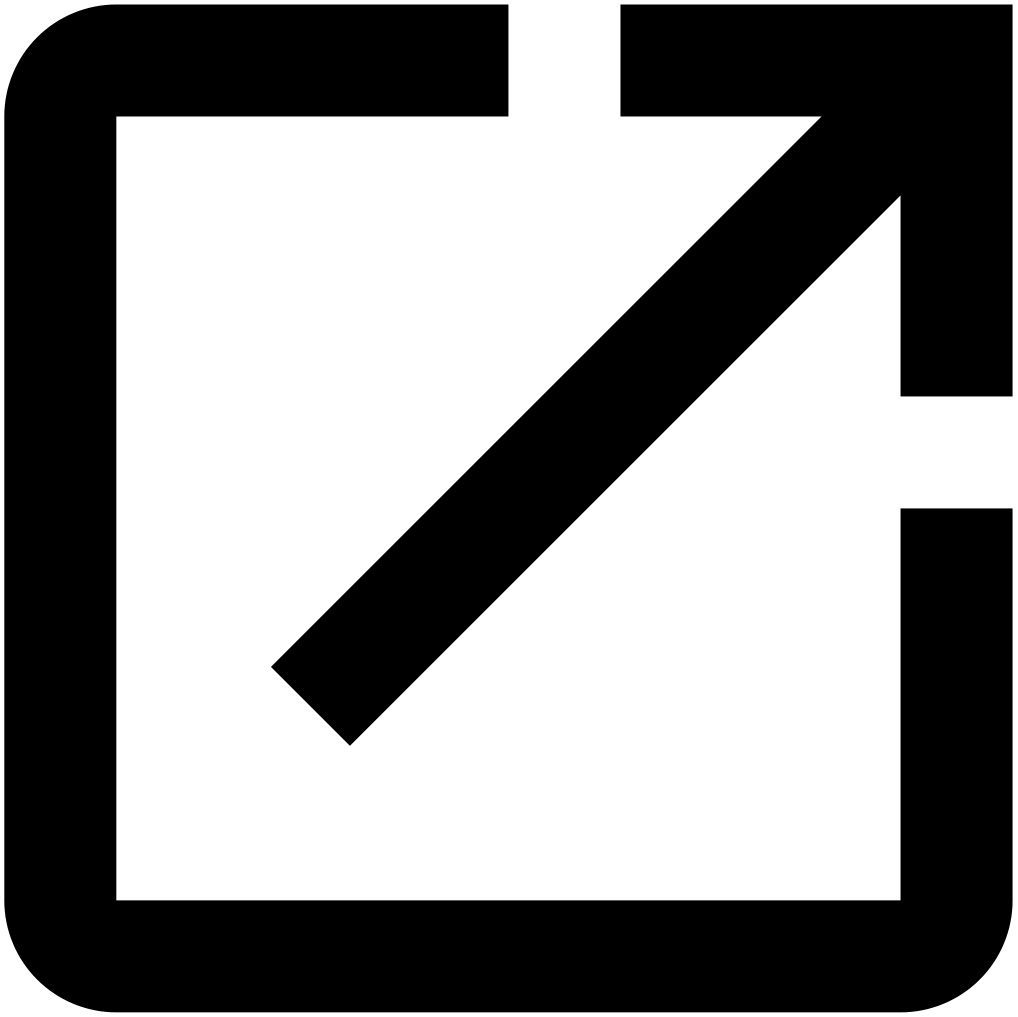


The infamous TrickBot trojan has started to check the screen resolutions of victims to detect whether the malware is running in a virtual machine.

When researchers analyze malware, they typically do it in a virtual machine that is configured with various analysis tools.

Due to this, malware commonly uses anti-VM techniques to detect whether the malware is running in a virtual machine. If it is, it is most likely being analyzed by a researcher or an automated sandbox system.


DIE LINKE.
0:00



These anti-VM techniques include looking for particular processes, Windows services, or machine names, and even checking network card MAC addresses or CPU features.

TrickBot uses screen resolution as anti-VM checks

In a new sample of the TrickBot Trojan discovered by cybersecurity firm MalwareLab's Maciej Kotowicz, the malware is now checking an infected computer's screen resolution to determine if it's a virtual machine.

Started as a banking Trojan, the TrickBot has evolved over time to perform a variety of malicious behavior.

This behavior includes spreading laterally through a network, stealing saved credentials in browsers, stealing Active Directory Services databases, stealing cookies and OpenSSH keys, stealing RDP, VNC, and PuTTY Credentials, and more.

In a tweet, Kotowicz stated that a new sample of TrickBot is checking if the computer's screen resolution is 800x600 or 1024x768, and if it is, TrickBot will terminate.

```
unsigned int __stdcall sub_8BB(api_ctx_t *a1)
{
  int v1; // ebx
  int v2; // eax
  unsigned int result; // eax

  v1 = ((int (__stdcall *)(_DWORD))a1->api_GetSystemMetrics)(0) << 16;// SM_CXSCREEN
  v2 = ((int (__stdcall *)(int))a1->api_GetSystemMetrics)(1);// SM_CYSCREEN
  result = tb_hash(0xAF65E7B8, v1 | v2);
  if ( result != 0x4A3C8992 && result != 0xC90692B8 )//
                                                // 800x600
                                                // 1024x768
    result = 0;
  return result;
```

TrickBot is checking for these particular resolutions because of how the researchers commonly configure their malware analysis virtual machines.

When configuring a virtual machine, most researchers will not install the VM guest software that allows for better screen resolutions, better mouse control, improved networking, and other features.

The software is not installed as malware commonly checks for files, registry keys, and processes used by the virtual machine guest software.

Without the guest software, though, a virtual machine will typically not allow any resolutions other than 800x600 and 1024x768, compared to ordinary screen resolutions that are much higher.

As an example, the popular free virtual machine software VirtualBox has a default resolution of 1024x768 when its guest additions software is not installed.

Advanced Intel's Vitali Kremez also told BleepingComputer that virtual machines used in automatic sandbox malware analysis solutions utilize this default resolution as well.

"Cuckoo VMs commonly have this exact resolution. Other sandbox engines such as JoeSandbox and Any App Run also rely on the exact same methodology with the default VM resolution," Kremez told BleepingComputer.

Knowing this, the TrickBot developers are using these screen resolution checks as another anti-VM check.

The good news is that if you are using these resolutions, you are safe from TrickBot. The bad news is that you are using these resolutions.
