Poorly coded Lamdelin Lockscreen Ransomware lets you in using Alt+F4

By AnandKhanse@TWC

Published: 2017-03-01 · Archived: 2026-04-05 14:44:14 UTC

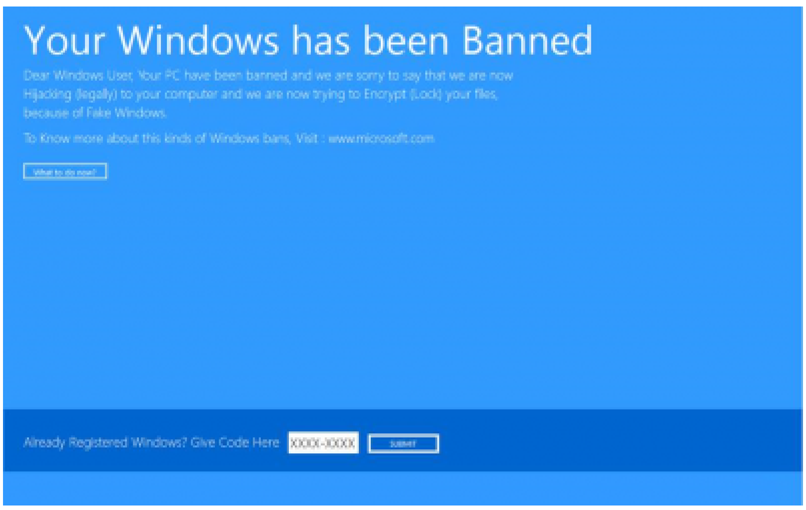
Ransomware, in general, is deadly, but sometimes their authors may not be intelligent enough to make them lethal enough, and that's what happened with the new Ransomware kid, **Lamdelim.A**.

Win32/Lamdelim.A has been detected as locking victim's PC in exchange for ransom. This lockscreen ransomware doesn't encrypt files like conventional Ransomware does, but it stops victims from accessing their data and demands $200 ransom for the unlock key. However, Lamdelin, at the same time is poorly coded, and those infected can break it and enter by simply using Alt+F4.

How Lamdelin Ransomware spreads

Lamdelin may catch you off guard by pretending itself to be a Microsoft file with name as "**microsoft.exe**" and using the icon below.

If you accidently execute "**microsoft.exe**" file, your PC screen is locked, and you get a message saying that "**Your Windows has been Banned**".



Lamdelin disables Task Manager by setting the following registry entry:

- In subkey: HKU\Administrator\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Sets value: “DisableTaskMgr”
- With data: “1” (REG_SZ)

The message asks for **$200 ransom**, to be paid to **“microsoftxyber[@]hackindex.com”.**

But, as mentioned above, you can recover from this attack successfully by following few simple steps.

Unlocking PC when infected with Lamdelin Lock screen Ransomware

Those infected can unlock their PC screen by entering a key that is found in the malware code, or simply closing the window by pressing **Alt+F4**. What puts Lamdelin’s author into a real shame is the fact that the unlock key is embedded in the malware code: **30264410**.

As soon as you enter 30264410, this threat displays a message – **“Windows Successfully Activated”**, which you can close using the X button:

As per Microsoft, PC users can also use the following free Microsoft tools to detect and remove this lockscreen Ransomware,

1. [Windows Defender]() for Windows 10 and Windows 8.1, or Microsoft Security Essentials for Windows 7 and Windows Vista
2. [Microsoft Safety Scanner]()
3. [Microsoft Windows Malicious Software Removal Tool]().

[Microsoft]() also recommends turning the Cloud-based Protection “On” as it checks latest malware threats.

Anand Khanse is the Admin of TheWindowsClub.com, a 10-year Microsoft MVP Awardee in Windows (2006-16) & a Windows Insider MVP (2016-2022). He enjoys following and reporting Microsoft news and developments in the world of Personal Computing.

Source: http://news.thewindowsclub.com/poorly-coded-lamdelin-lockscreen-ransomware-alt-f4-88576/