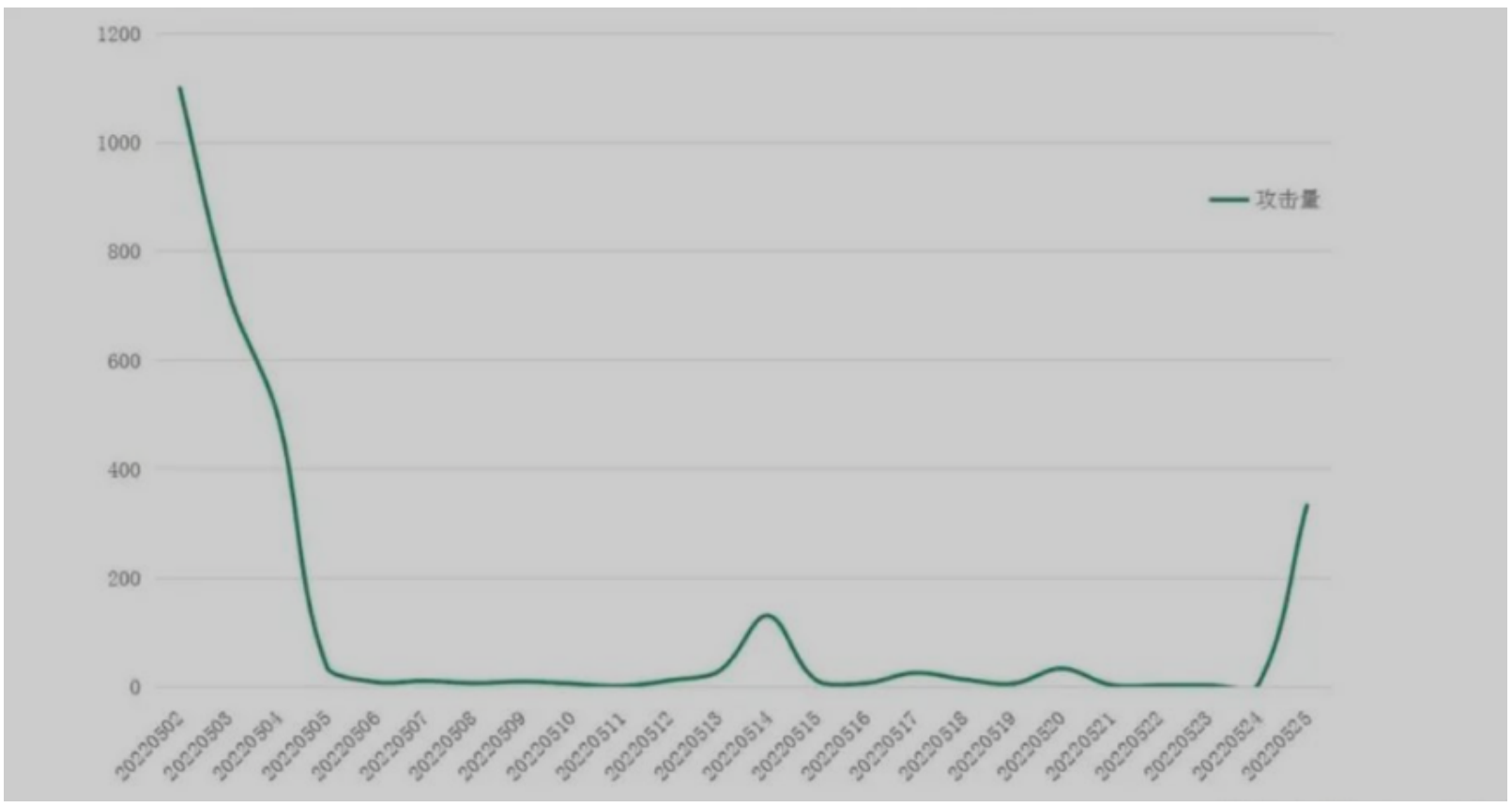
Win11 users beware! Magniber ransomware has been upgraded again, aiming at win11

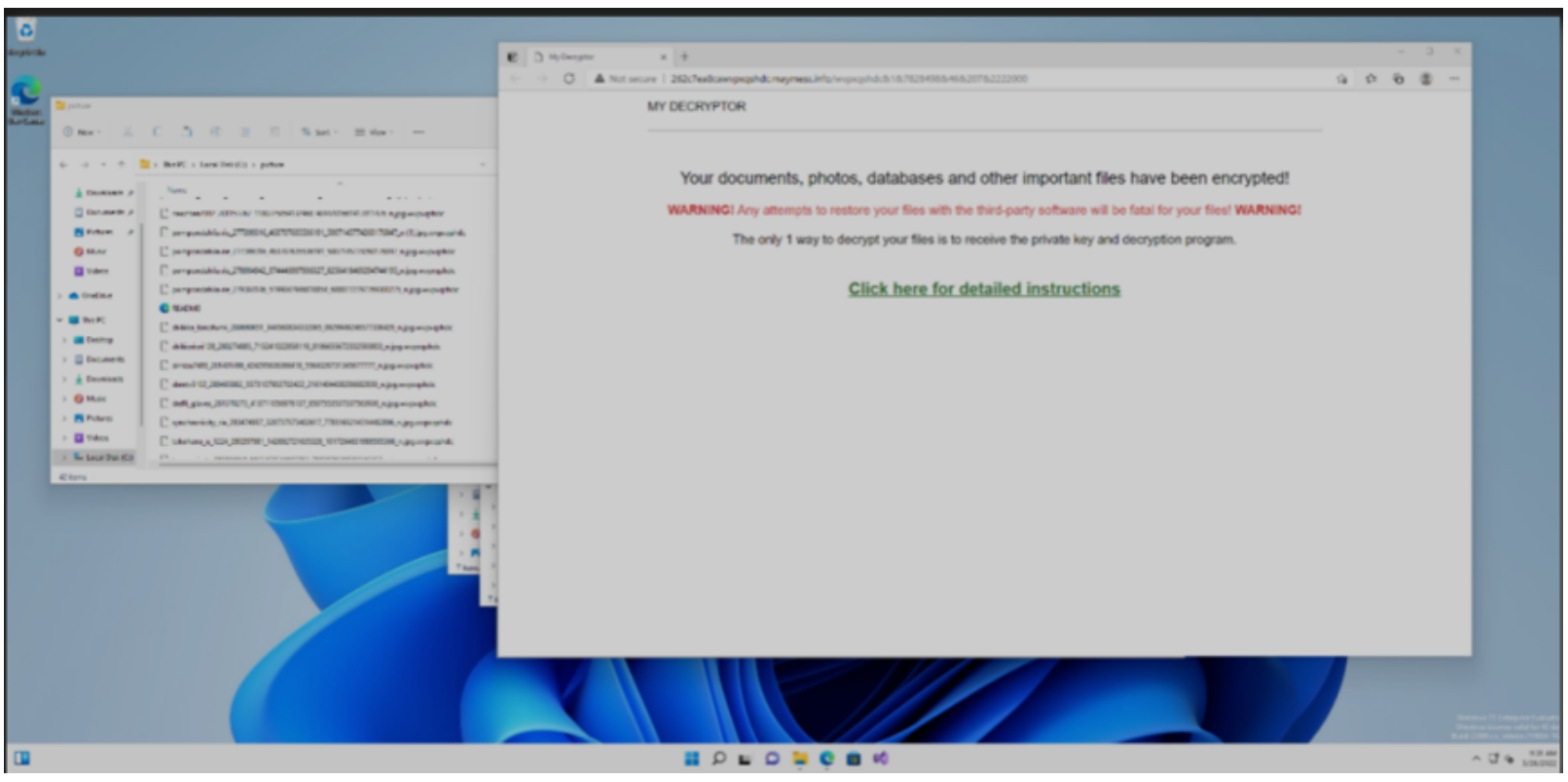
May 27, 2022kate Choose a language Learn more about 360 Total Security

At the end of April this year, the Magniber ransomware disguised as a Windows 10 upgrade patch package and spread widely, and 360 Security Center warned it. Just recently, 360 Security Center detected a new attack on the Windows 11 system in the family. Since May 25, its attack volume has increased significantly, and its main dissemination package names have also been updated, such as: win10-11_system_upgrade_software.msi, covid.warning.readme.xxxxxxxx.msi, etc.

The transmission method is still various forums, cracked software websites, fake pornographic websites, etc. When users visit these websites, they are induced to download from third-party network disks. The recent spread of the virus is as follows:

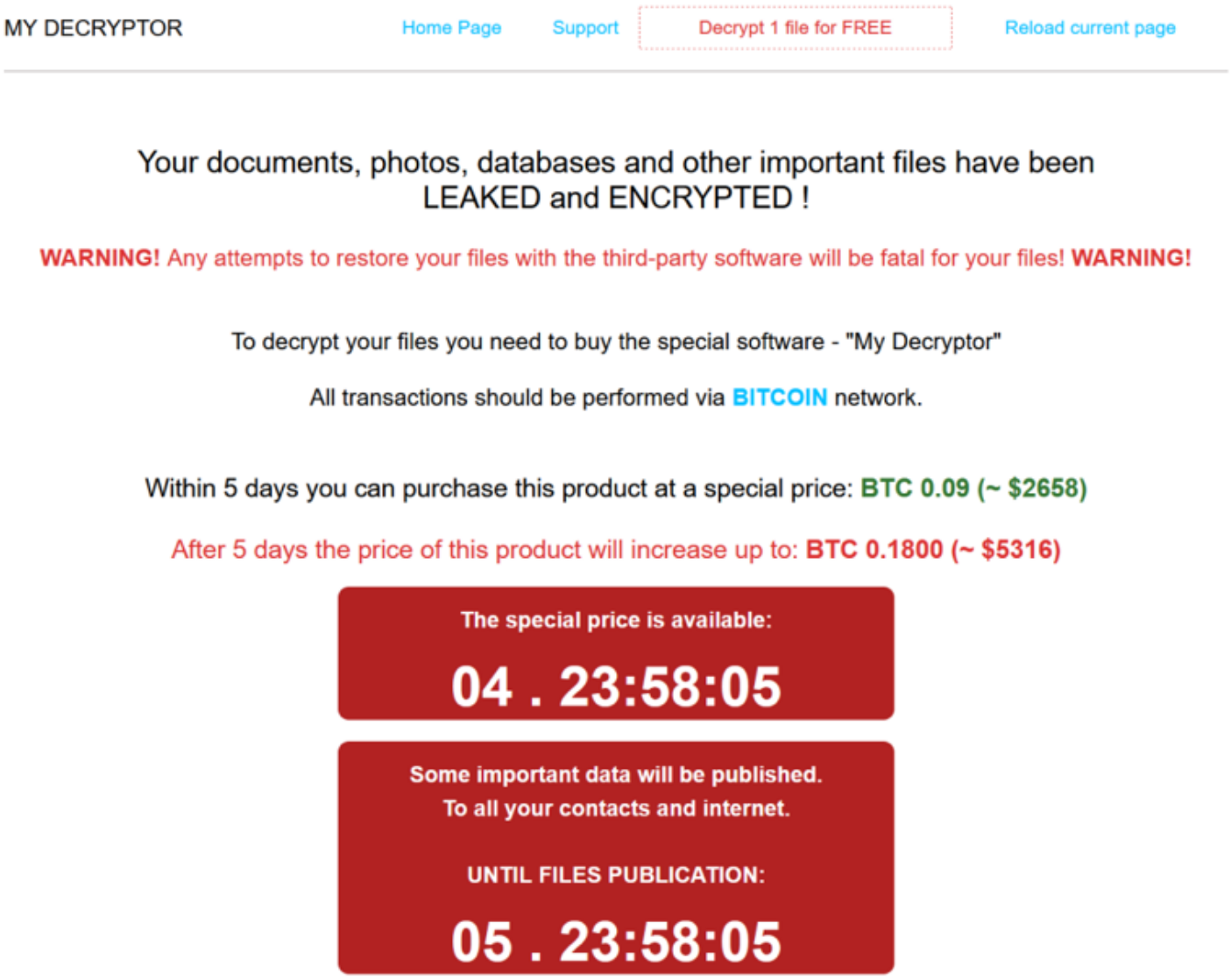


The virus program itself has not changed much, and can infect multiple versions of Windows operating systems. The following figure shows the scene of Windows 11 being infected by the virus.

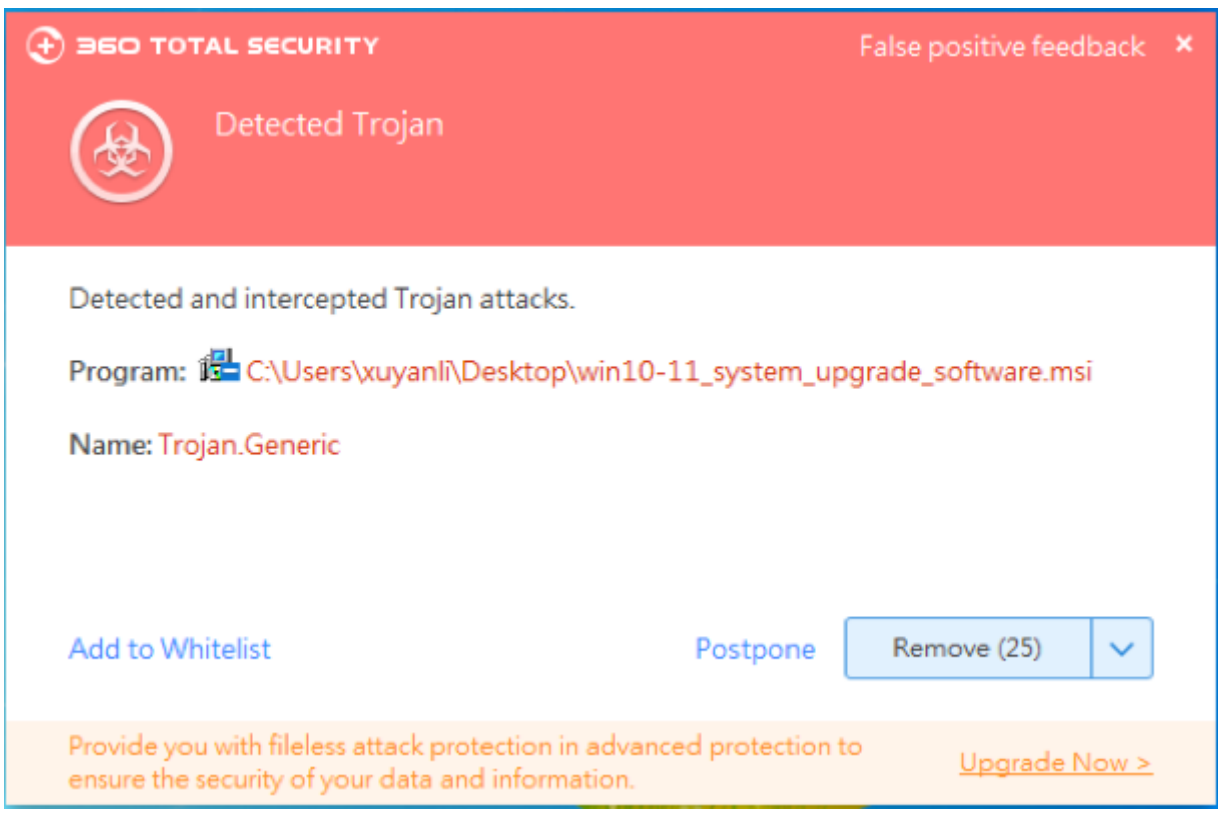


The virus uses the RSA+AES encryption scheme when encrypting files. The RSA used is as long as 2048 bits, which is currently difficult to crack technically.

After being encrypted by the ransomware, the file suffix is a random suffix, and each victim will have an independent payment page. If the ransom cannot be paid within the specified time, the link will be invalid. If the victim can pay the ransom within 5 days, he only needs to pay 0.09 Bitcoin, and the ransom will be doubled after 5 days.



At present, 360 Total Security can support the interception and killing of the ransomware virus. It is recommended that users do not run unknown programs downloaded from unknown websites at will.



IOC (part)

hxxps://casbin[.]info/campid=18

hxxps://flatis[.]uno/src=6584

hxxps://agorule[.]fun/src=98411

hxxps://vocoto[.]info/src=1990

2e29176531e8c9f9fe10ca6f11d6ba33

6d50b91f8f9811ce287bdfda686e5d96

3947a4b4b888831be48251323611cbdd

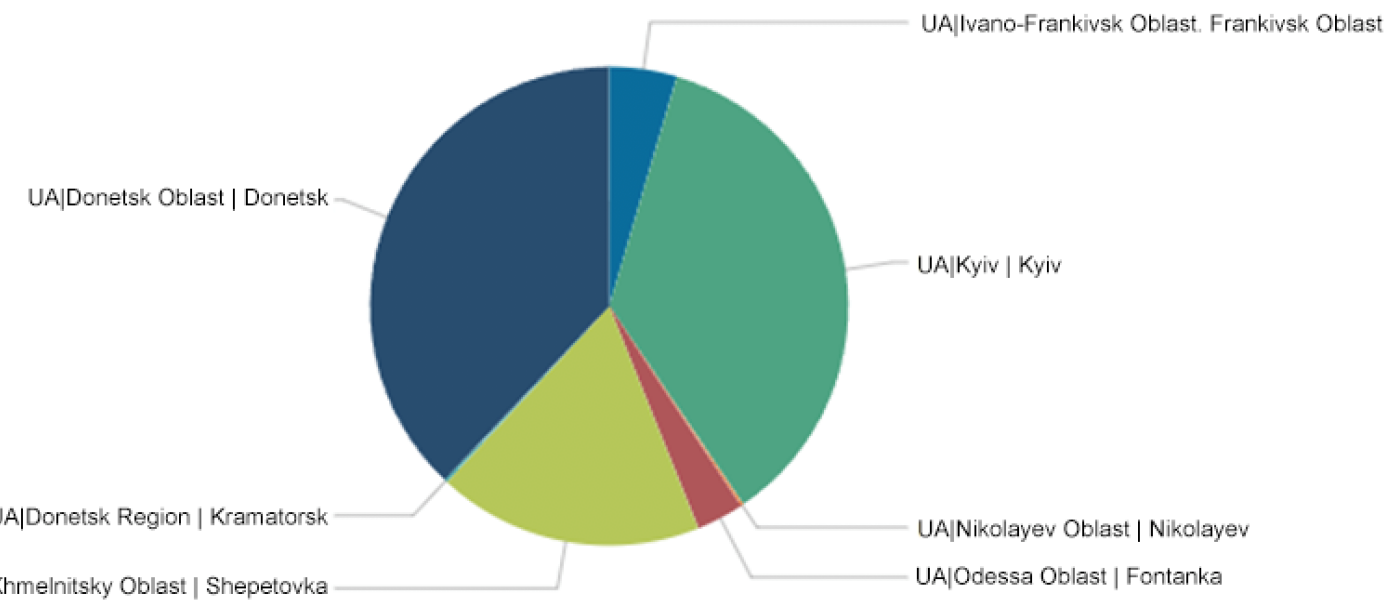
8206b320422149d45096ae9a13acfcc5

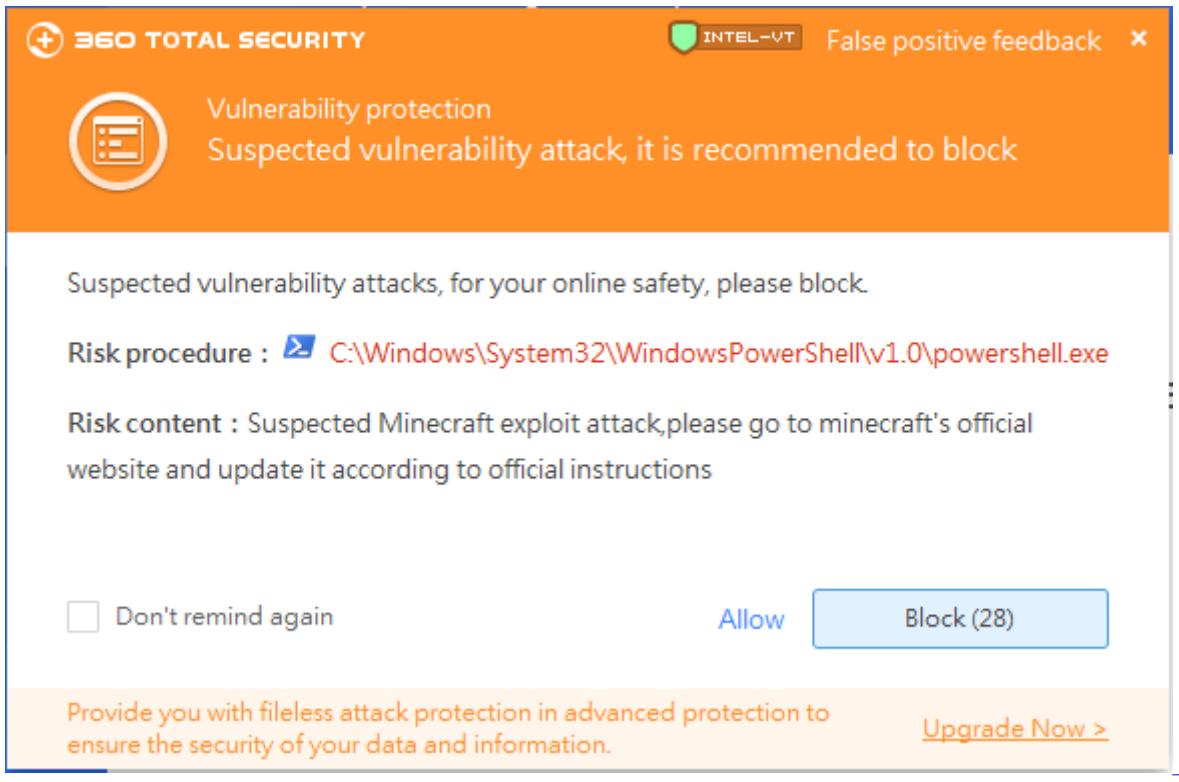
0163f2973f37fcb176b6f642ce0aca3d

Learn more about 360 Total Security Share:

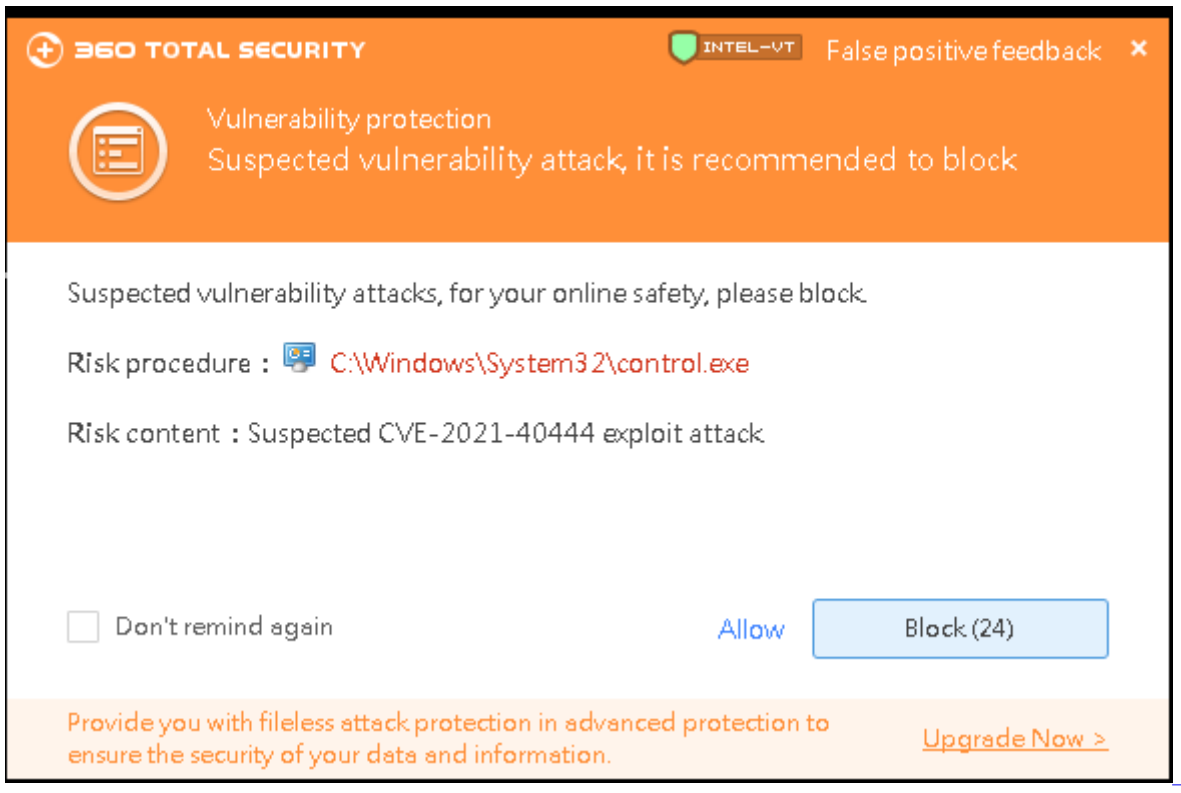
-

Related Articles

- 

Exclusive in-depth analysis: directly attack the key technical details of Ukraine's cyber warfare
- 

Urgent! Minecraft players are under massive attack
- 
Urgent | Apache log4j-2.15.0-rc1 version has a bypass risk, please upgrade to log4j-2.15.0-rc2 as soon as possible!

- 

No patch available for the Microsoft Windows MSHTML remote code execution vulnerability, 360 Total Security takes the lead to intercept it!