Microsoft maintains the recovery key of your new PC

December 29, 2015 By Pierluigi Paganini

If you login to Windows 10 using your Microsoft account you have to know that your computer automatically uploaded a copy of your recovery key.

New Windows computers implement a built-in disk encryption feature that is turned on by default to protect user data in case the device is lost or stolen.

Be aware, this device encryption feature is different from the BitLocker which allows users to choose whether or not to backup their Recovery keys on Windows server.

The security feature is enabled by default in Microsoft systems since Windows 8.1, but what happen in case the user lost the encryption keys?

Microsoft maintains a copy of the Recovery Key, a circumstance that is raising a heated debate on the

The Intercept revealed that when a user is logged into Windows 10 using his Microsoft account, the OS automatically uploads a copy of the recovery key to the Microsoft's servers, and the bad news is that it is impossible to prevent it.

"But what is less well-known is that, if you are like most users and login to Windows 10 using your Microsoft account, your computer automatically uploaded a copy of your recovery key – which can be used to unlock your encrypted disk – to Microsoft's servers, probably without your knowledge and without an option to opt-out." ***states*** The *Intercept.*

Clearly this setting open users to a number of cyber attack, let's think the case an attacker violates their Microsoft account, he would be able to access/copy the recovery key and delete it. A similar circumstance could occur if hackers compromise Microsoft servers and access the recovery keys of the users, or if an insider access to user recovery key.Even Law Enforcement or Spy agencies could also request Microsoft to hand over your recovery key.

Even law enforcement or intelligence agencies could force Microsoft to hand over the recovery key of a suspect.

"Your computer is now only as secure as that database of keys held by Microsoft, which means it may be vulnerable to hackers, foreign governments, and people who can extort Microsoft employees," said Matthew Green, a cryptography professor at Johns Hopkins University.

The Intercept highlighted that storage of the recovery key on Microsoft's servers makes the company an escrow agent, users can delete their recovery key, but they are not informed about this opportunity.

"The fact that new Windows devices require users to backup their recovery key on Microsoft's servers is remarkably similar to a key escrow system, but with an important difference. Users can choose to delete recovery keys from their Microsoft accounts

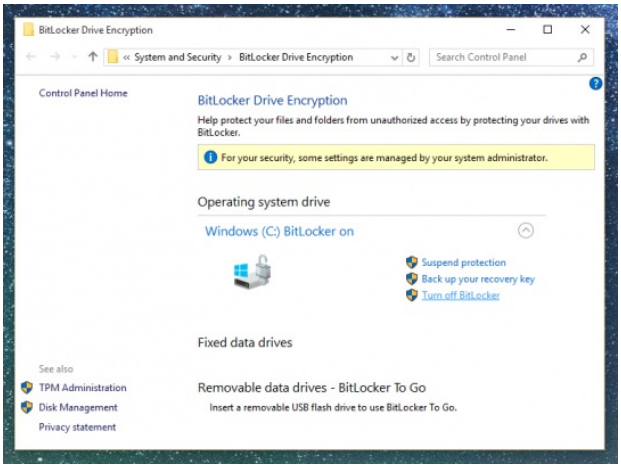
(you can skip to the bottom of this article to learn how) – something that people never had the option to do with the Clipper chip system. But they can only delete it after they've already uploaded it to the cloud.

How to Delete the Recovery Key from a Microsoft Account?

We said that it is not possible to prevent a new Windows computer from uploading the key at the very first time you log into your Microsoft account, you can delete the existing one from your Microsoft account and generate a new one.

Below the procedure to remove the encryption key from a Microsoft account:

- Login in using the Microsoft Account to the Recovery Key Website:
- The website maintains a list of recovery keys backed up to your Microsoft Account.
- Backup Recovery Keys locally.
- Delete the recovery key from the Microsoft Account.



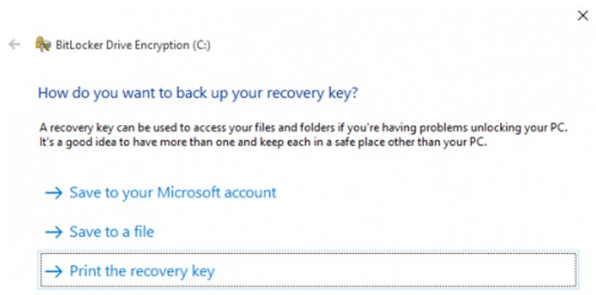
The Intercept highlighted that even following the above procedure there is no guarantee that the key has been removed from the Microsoft servers, the unique possibility for the user is to generate a new recovery key without uploading it to Microsoft.

"After you finish setting up your Windows computer, you can login *to your Microsoft account and delete the recovery key. Is this secure enough? "If Microsoft doesn't keep backups, maybe," says Green. "But it's hard to guarantee that. And for*

people who aren't aware of the risk, opt-out seems risky."

Windows Pro or Enterprise users can create a new key by decrypting the hard disk and then re-encrypt the disk, below the procedure to do it.

1. Go to Start, type "bitlocker", and click "Manage BitLocker."
2. "Turn off BitLocker," this command will trigger the decrypt of the entire disk.
3. Once completed, Click "Turn on BitLocker" again.
4. The OS will request you how to backup the Recovery Key. Make sure to DO NOT SELECT "Save to your Microsoft Account."



That's all!

Pierluigi Paganini

(Security Affairs – encryption, Microsoft)

Microsoft | encryption | Recovery Key | BitLocker

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE
A new emergency patch for Adobe Flash Zero-Day, update your system!

NEXT ARTICLE
Former Employee tried to sell Yandex Source Code for Just $29K

YOU MIGHT ALSO LIKE

Is Play Station Network under attack? Users reported issues

December 25, 2015 By Pierluigi Paganini

Phantom Squad plans to hack PSN and Xbox, SkidNP hacks its website

December 20, 2015 By Pierluigi Paganini

- +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group,

he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

Back to top