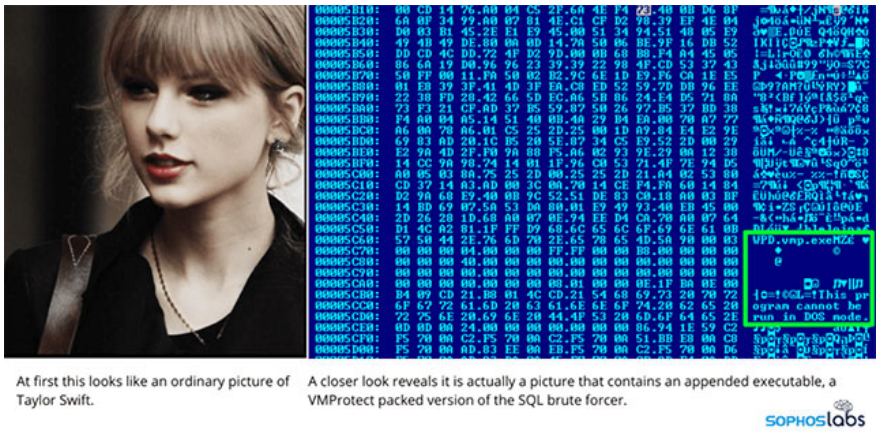
Detecting cryptocurrency mining Botnet using photos of Taylor Swift to spread malicious code

This botnet is called MyKingz (also known as Smominru, DarkCloud or Hexmen).

UK-based cybersecurity firm Sophos, has just found a cryptocurrency mining botnet that has a unique and effective way to spread malicious code.

This botnet, called MyKingz (also known as Smominru, DarkCloud or Hexmen), now takes advantage of steganography - a technique that allows hiding malicious files inside valid files to trick people 'lightly. gullible 'or not very knowledgeable about data security.

According to Sophos' discovery, the people behind MyKingz had hidden a malicious EXE executable file inside the JPEG image of famous singer Taylor Swift and used this image to deceive and spread the malicious code on. computers of the victims when they click on the photo.



The original image (left) looks very normal, but deep inside it is a malicious file

Actually, MyKingz is not a new Botnet. It was first discovered in 2017, but one of the characteristics that makes MyKingz so dangerous is its ability to hide and change the mode of transmission extremely flexible. Currently, this Botnet is recognized as one of the few malware exploiting cryptocurrency with scale up to hundreds of thousands of devices.

In actual operation, MyKingz mainly focuses on Windows systems, and in particular, this Botnet owns one of the most sophisticated scanning and malware infection mechanisms ever recorded on all botnets. known to the present time. MyKingz can target any Windows-related system, such as MySQL, MS-SQL, Telnet, ssh, IPC, WMI, Remote Desktop (RDP) and even storage servers. CCTV camera.

According to estimates, just a few months after being launched on a global scale, MyKingz successfully infected over 525,000 Windows systems, collecting Monero virtual currency (XMR) worth up to more than $ 2.3 million. . The 'preferred' countries of this Botnet include: China, Taiwan, Russia, Brazil, USA, India and Japan.

Sophos' latest report shows that MyKingz is currently infected with around 4,700 new systems and helping attackers pocket $ 300 a day - the amount is not too large but mainly because Monero's exchange rate is on the decline. strong.