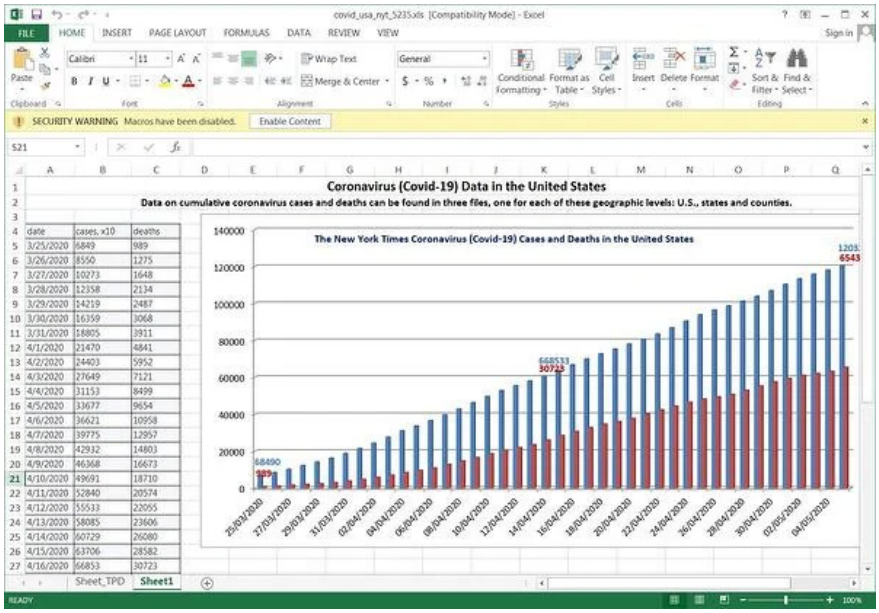
Microsoft urgently warns about a phishing campaign that uses malicious Excel macros to hack PCs

Security team with Microsoft's Security Intelligence has issued an urgent warning about a massive fraud campaign.

Security team with Microsoft's Security Intelligence has issued an emergency warning about a "massive" fraud campaign that could affect the millions of Microsoft users they've been following for days. In this campaign, the hacker will try to install the remote access tool on the target PC by tricking the victim into opening an email attachment containing a malicious Excel 4.0 macro.

According to the results of Security Intelligence's investigation, this fraudulent campaign 'follows' the hot topic currently translated as COVID-19. It started being deployed on May 12 and has so far spread hundreds of malicious, well-designed attachments to the internet environment. These malicious files will often be included in fake fake emails, from reputable sources like WHO, Johns Hopkins Center and other international public health organizations.

If the recipient tries to open the attached malicious Excel files, he or she will see the content displayed as a security warning and a chart of COVID-19 infections around the world. But if allowed to run, the malicious Excel 4.0 macro will download itself and run a program called NetSupport Manager.



Malicious Excel file

Basically, NetSupport Manager is a legitimate remote access tool, but in this case, it can be abused by an attacker to gain remote access to the target computer, then customize it. intentionally run malicious commands on compromised systems, Security Intelligence warns.

'In the past few months, we have noticed a steady increase in the use of malicious Excel 4.0 macros in many malware attack campaigns. The Excel 4.0 campaigns have shown signs of booming since the beginning of April and mostly follow the theme of COVID-19 '.

- Microsoft Security Intelligence

Notably, although hundreds of malicious files have been distributed and tampered with in various attacks, they all connected to the same URL to download malicious payloads to the system. infected.

Recently, TipsMake also had a number of articles warning readers about the situation of hackers actively taking advantage of the complicated evolution of the COVID-19 epidemic to deploy online fraud and spread malware. on a global scale. In late April, Google said it successfully blocked millions of malicious COVID-19-related emails on Gmail every day.

In general, the form of malicious phishing attachments in emails has been designed more sophisticatedly but it is not new in nature. Even so, it will still be dangerous for ordinary users who do not have a lot of security knowledge.

You can turn off macros in Excel if you do not use this feature to prevent risks.