Discover the new malicious code, automatically record the victim's screen when they watch 'adult movies'

Yes, a finding may shock the global FA world.

Yes, a discovery could make "global FA shocks". Recently, security - network security researchers from ESET antivirus software development company have discovered a new malware, distributed in the form of spam email, relatively 'interesting', In addition to the ability to steal user data such as passwords and personal financial information stored on the device, this malicious code is also equipped with the ability to record the victim's screen whenever they see it. Erotic content on adult sites.

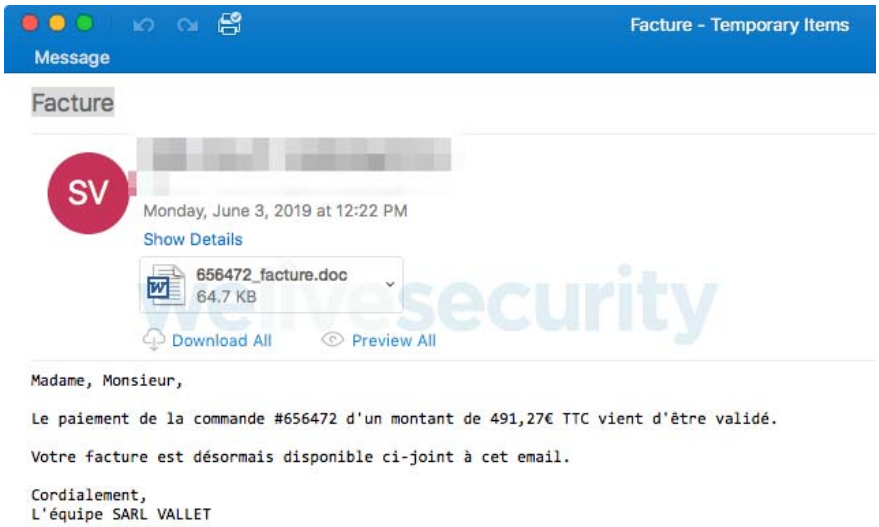
This virus is called Varenyky and it is a doozy (unusual type of malicious code). According to the researchers' analysis, the malware was originally designed to target a single target: customers of French telecommunications group Orange SA - this may be part of the campaign. Some unfair competition targets this huge telecommunications group. However, the team also found that nothing could prevent an individual from using this malware and targeting other organizations or individuals, or even spreading malicious code. widespread.

1. Even DSLR cameras can be easily attacked by ransomware

Varenyky was originally designed to target customers of Orange SA

Code of Varenyky possesses a traditional method of spread, nothing new, but still extremely effective, in the form of spam emails. The email containing malicious code will be extremely sophisticated camouflage, looks very much like a phone bill, or a notification from the network sent to the customer. And if you accidentally click on the link or download the malicious media file attached to that email - congratulations! You have joined the 'club' victims of Varenyky.

1. Stealing, electronic money scams in 2019 may hit a record of $ 4.3 billion



The spam email containing Varenyky is extremely camouflaged

The way the virus spreads into the system is nothing special. Usually Varenyky is included in a very good camouflage file, usually like a Word file, making the victim think that the document was censored and confidential by Microsoft, while in fact they were unknowingly. Activate the virus and allow it to penetrate the macro in Word. Specifically follow a post on the ESET website as follows:

"In general, the contents of email attachments, document file names and content protected by vendors are sophisticatedly disguised, to emphasize to the recipient that they are processing a real email, and should open it for more information The quality of the deceive text written in French is also very good, without semantic and grammatical errors In general, this malicious document looks very convincing, which can make those People who are most cautious can make mistakes. "

Once enabled, the attached macro in the fake text will automatically execute processes that allow the malware to download additional files needed to collect passwords, transfer them to other systems, and write back to the victim's screen without them knowing.

After obtaining valuable private information, the attacker will play cards face-to-face and send an e-mail in English. This email was discovered and published by the ESET team, with the following content:

1. Air New Zealand hacked, customer information is at risk of falling into the hands of hackers

Information

You may not know me and you are probably wondering why you are getting this e mail, right?
I'm a hacker who cracked your devices a few months ago.
I sent you an email from YOUR hacked account.
I setup a malware on the adult vids (porno) web-site and guess what, you visited this site to have fun (you know what I mean).
While you were watching videos, your internet browser started out functioning as a RDP (Remote Control) having a keylogger which gave me accessibility to your screen and web cam after that, my software program obtained all of your contacts and files.

You entered a passwords on the websites you visited, and I intercepted it.

Of course you can will change it, or already changed it.
But it doesn't matter, my malware updated it every time.

What did I do?
I created a double-screen video. 1st part shows the video you were watching (you've got a good taste haha . . .), and 2nd part shows the recording of your web cam.
Do not try to find and destroy my virus! (All your data is already uploaded to a remote server)
– Do not try to contact with me
– Various security services will not help you, formatting a disk or destroying a device will not help either, since your data is already on a remote server.

I guarantee you that I will not disturb you again after payment, as you are not my single victim.
This is a hacker code of honor.

Don't be mad at me, everyone has their own work.
exactly what should you do?

Well, in my opinion, $[illegible] (USD) is a fair price for our little secret. You'll make the payment by Bitcoin (if you do not know this, search "how to buy Bitcoin" in Google).

My Bitcoin wallet Address:

[illegible]

(It is cAsE sensitive, so copy and paste it, you can use **Bitpay.com** for QR code payment)

Important:
You have 48 hour in order to make the payment.
(I've a facebook pixel in this mail, and at this moment I know that you have read through this email message).
To track the reading of a message and the actions in it, I use the facebook pixel.
Thanks to them. (Everything that is used for the authorities can help us.)
If I do not get the Bitcoins, I will certainly send out your video recording to all of your contacts including relatives, coworkers, and so on. Having said that, if I receive the payment, I'll destroy the video immediately.

The message of extorting victims and instructing how to pay ransom

It can be seen that hackers blackmail victims by saying they have obtained valuable personal data from them, as well as recording the times they visited the adult site. The victim will have to choose to pay or let the information be publicly available, as well as send to all colleagues, relatives and friends of the victim to discredit them. At the same time, crooks also give detailed instructions on how victims can transfer money to them. The victim will have to convert cash to Bitcoin and send it to the e-wallet address provided by them.

So how dangerous is this malicious code? When this 'sextortion' scam aspect (this tactic of attacking users with sensitive photos or videos) in fact does not seem to be a big threat. Security expert Bruce P. Burrell, head of the research team, said the hacker behind this case is using a sextortion scam kit he bought on the dark web. Up to now, no case has been recorded by Varenyky under this method, and experts say the problem is not really about watching pornography recorded. again.

1. Alarming statistics on the situation of network security in our country in the first half of 2019

The tactics of attacking users with sensitive photos or videos of malicious code Varenyky is not the biggest threat

People who have accidentally downloaded fake invoices and given the wrong permissions to run macros are at risk of getting stolen passwords and very high financial information, as well as continuing to spread malware to others in Their contact list. That is the main issue!

Although Varenyky is unlikely to be a global threat, and so far, there has not been any record that it has succeeded in extorting any individual, but the simplicity of the attack vector This malicious code is worth noting.

On the other hand, ESET's research team also believes that the malware developers behind Varenyky are 'tenacious and highly skilled':

"Many functions have been added and then quickly deleted on different versions of malicious code in a relatively short period of time (2 months). This shows that malware operators still are actively developing their botnet, and tend to increase the testing of more new features so that malicious code can bring better money for them. '

1. *What is email encryption? Why does it play an important role in email security?*

Although Varenyky has not spread widely and become a global threat, this is not impossible, so each individual should still know how to protect himself. Security experts say the best way to prevent malware is to always update your operating system and antivirus software to the latest version, and especially avoid opening email attachments or downloading them. Strange files unless you're 100% sure they're not dangerous.

and for following us regularly.