Discovered that a fake PayPal website is spreading Nemty Ransomware

The spread of Nemty malware has been closely observed by security experts on the fake PayPal website.

International security researchers recently discovered a fake website, disguised as an address that provides some official applications from PayPal, but actually spread a new variation of the code. poisoned Nemty extortion, making many gullible people become victims of this dangerous ransomware.

It seems that the people behind this data encryption malware are trying to test various malware distribution channels because recently security experts have discovered its trace as a payload from a RIG exploit kit (EK).

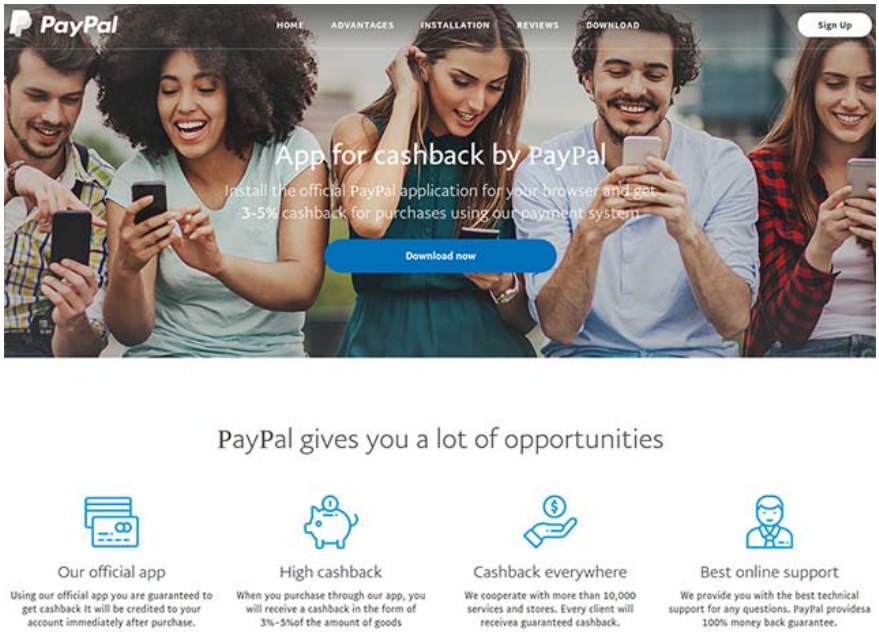
1. French police successfully cracked down on a botnet that exploits 850,000 computers from more than 100 countries.

Nemty ransomware is being distributed through a fake website

Sophisticated method of deception

The spread of Nemty malware has been closely observed by security experts on the fake PayPal website, including a proposal that promises to give customers 3% to 5% of the amount from Purchases are successfully made through the payment system. According to experts, this attractive proposal is an attractive bait, hitting the greed of many people and making them victims of malicious code without even knowing it.

1. Discovered new malware, automatically recording a victim's screen when they watch 'adult movies'

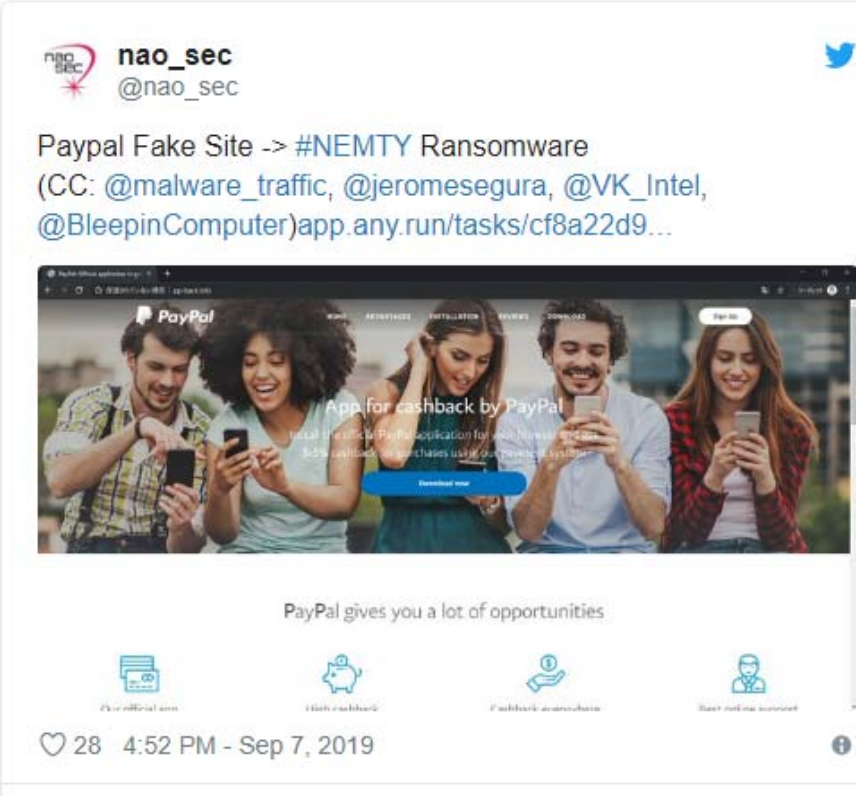


The fake PayPal website is very similar

It is not too difficult for researchers to find clues about the fraudulent nature of this fake website. Besides, it is also marked as dangerous by most popular browsers. However, the fact that the proposed content, the often attractive amount of money that crooks still make many people ignore all warnings, just download and launch malware on your system. It is known that the executable file contains a malicious code called 'cashback.exe'.

Security researcher nicknamed nao_sec found the distribution channel of this Nemty malware, and used the AnyRun test environment to deploy malware and track all its activity on an infected system. infected.

1. Even DSLR cameras can easily be attacked by ransomware



Security researcher nicknamed nao_sec found the distribution channel of the Nemty malware

The automated analysis showed that it took about 7 minutes for the malicious code to finish encrypting the entire file on the victim server. Of course it still depends on the amount of data that the victim owns, but 7 minutes is the average period.

Fortunately, this malicious software can be detected by most commonly used antivirus programs on the market today. The scan results on VirusTotal show that up to 36 of the 68 most popular antivirus engines can now detect malicious signs of executable file 'cashback.exe'.

1. After 15 years, the infamous MyDoom worm still exists and threatens email users worldwide

Homoglyph attack

At first glance, this malicious website is very similar to the real one because hackers have used images, interface structure, as well as information layout quite similar to the usual websites of PayPal.

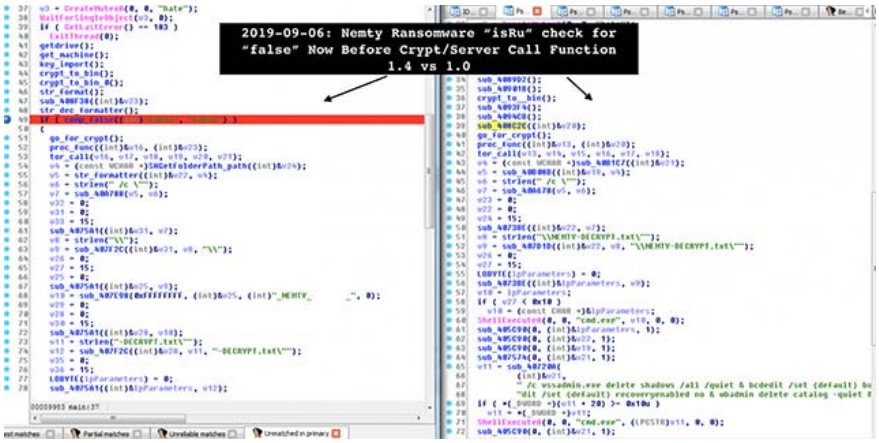
Not only that, in order to create more trust for the victims, the fake website developers have used a 'technique' called fake homograph domain names for links that lead to different sections of the site. web, such as Help & Contact, Fees, Security, Apps, and Shop .

Crooks have developed this sophisticated technique by using domain Unicode characters from various alphabets. To distinguish between them, browsers will automatically translate them into Punycode. In this case, the characters in Unicode that look like paypal.com are translated into 'xn--ayal-f6dc.com' in Punycode.

Security researcher Vitali Kremez conducted an analysis of this Nemty ransomware variant and noted that it is currently in version 1.4, along with some minor bug fixes.

The researchers paid special attention to a test procedure called 'isRU'. 'isRU' helps to verify whether computers infected with malware in some CIS countries such as Russia, Belarus, Kazakhstan, Tajikistan or Ukraine, have been modified. 'In the latest version, if the test result is' positive', the malware does not come with a file encryption function, " said Vitali Kremez.

1. No More Ransom - the flagship of the battle against ransomware



Security researcher Vitali Kremez conducted an analysis of the Nemty ransomware variant

However, countries outside this region will still be a lucrative target for malicious code. That is, they can still encrypt the file system as well as delete the virtual backup on the victim's system as usual.

The name Nemty ransomware has been a topic of discussion on many international security forums for a long time, but it was only really put on the watchlist of the infosec community at the end of August, at a time when Security researcher Vitali Kremez details his malware analysis process.

Also around the end of August, another security researcher, nicknamed Mol69, discovered that the Nemty malware was distributed via RIG EK, this is probably a strange choice in the context of the ministries. Mining tools are on the brink of 'extinction' when they target products that are related to an unpopular browser platform: Internet Explorer, Flash Player.

1. Ransomware is showing signs of booming around the world, and paying is no longer the most viable option.

According to security expert Yelisey Boguslavskiy of Advanced Intelligence, Nemty is an emerging ransomware strain, not too dangerous but still capable of causing great damage if the measures to prevent the spread of malicious code are not taken from early.