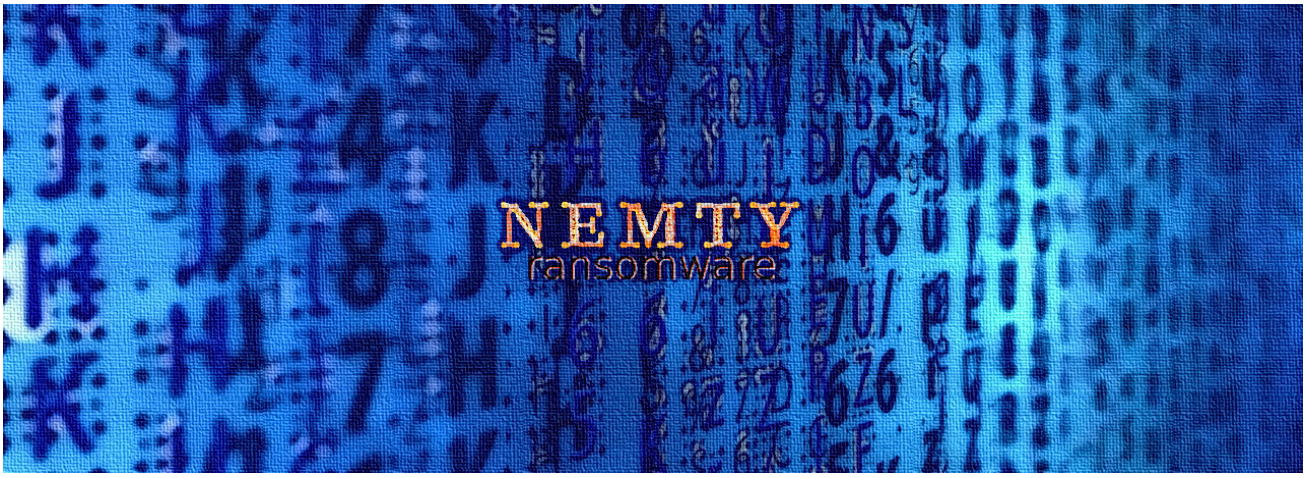
Fake PayPal Site Spreads Nemty Ransomware

bleepingcomputer.com/news/security/fake-paypal-site-spreads-nemty-ransomware/

Ionut Ilascu

By
Ionut Ilascu

- September 8, 2019
- 11:01 AM
- 0

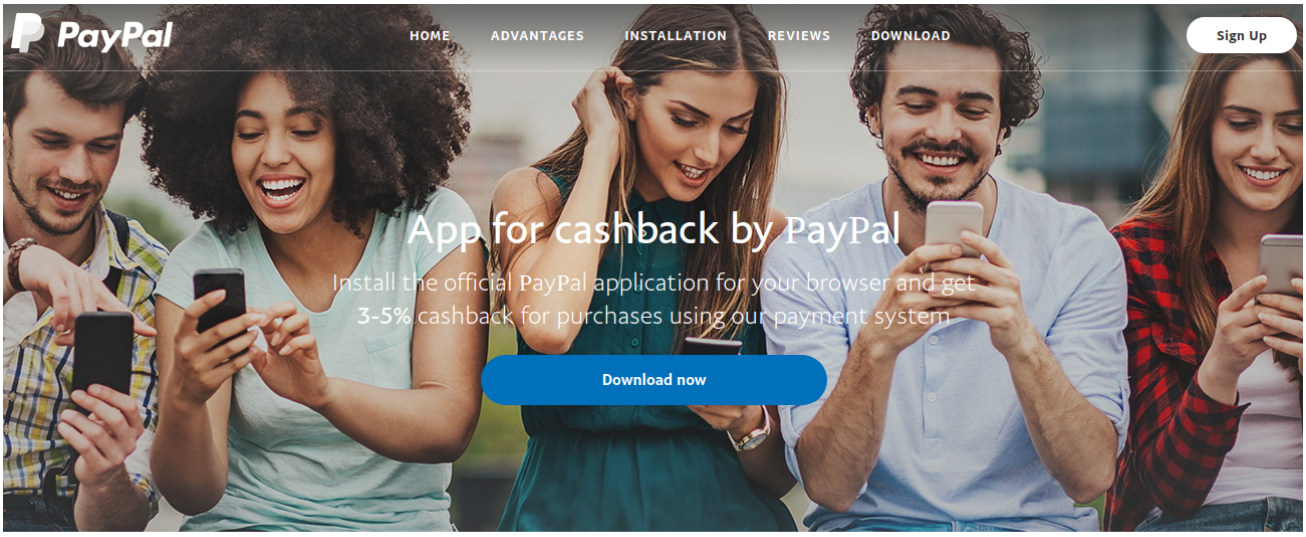


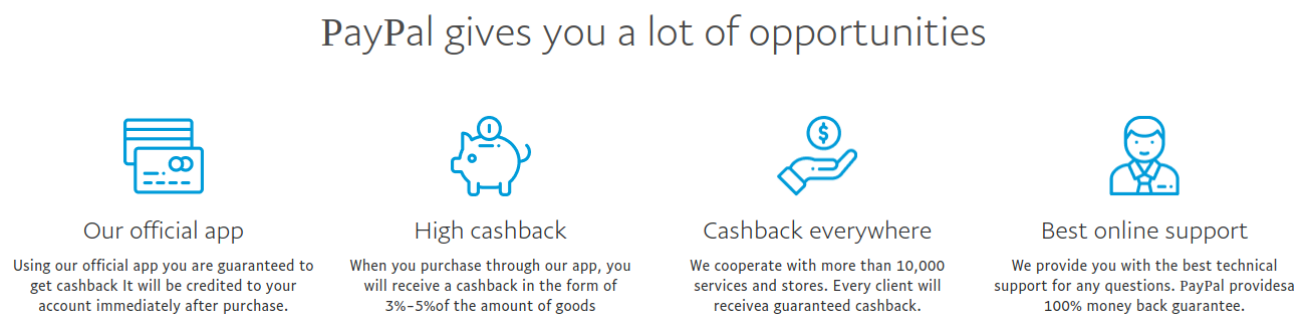
A web page pretending to offer an official application from PayPal is currently spreading a new variant of Nemty ransomware to unsuspecting users.

It appears that the operators of this file-encrypting malware are trying various distribution channels as it was recently observed as a payload from the RIG exploit kit (EK).

Luring with cashback rewards

The latest occurrence of Nemty was observed on a fake PayPal page that promises to return 3-5% from purchases made through the payment system.





Several clues point to the fraudulent nature of the page, which is also flagged as dangerous by major browsers, but users may still fall for the trick and proceed with downloading and running the malware, which is conveniently named 'cashback.exe'.

Security researcher nao_sec found the new Nemty distribution channel and used AnyRun test environment to deploy the malware and follow its activity on an infected system.

> Paypal Fake Site -> #NEMTY Ransomware
> (CC: @malware_traffic, @jeromesegura, @VK_Intel,
> @BleepinComputer)https://t.co/YC7pVMSFwm pic.twitter.com/yzakaFEzi0
>
> — nao_sec (@nao_sec) September 7, 2019

The automated analysis showed that it took about seven minutes for the ransomware to encrypt the files on the victim host. However, this may differ from one system to another.

Fortunately, the malicious executable is detected by most popular antivirus products on the market. A scan on VirusTotal shows that it is detected by 36 out of 68 antivirus engine.

Homoglyph attack

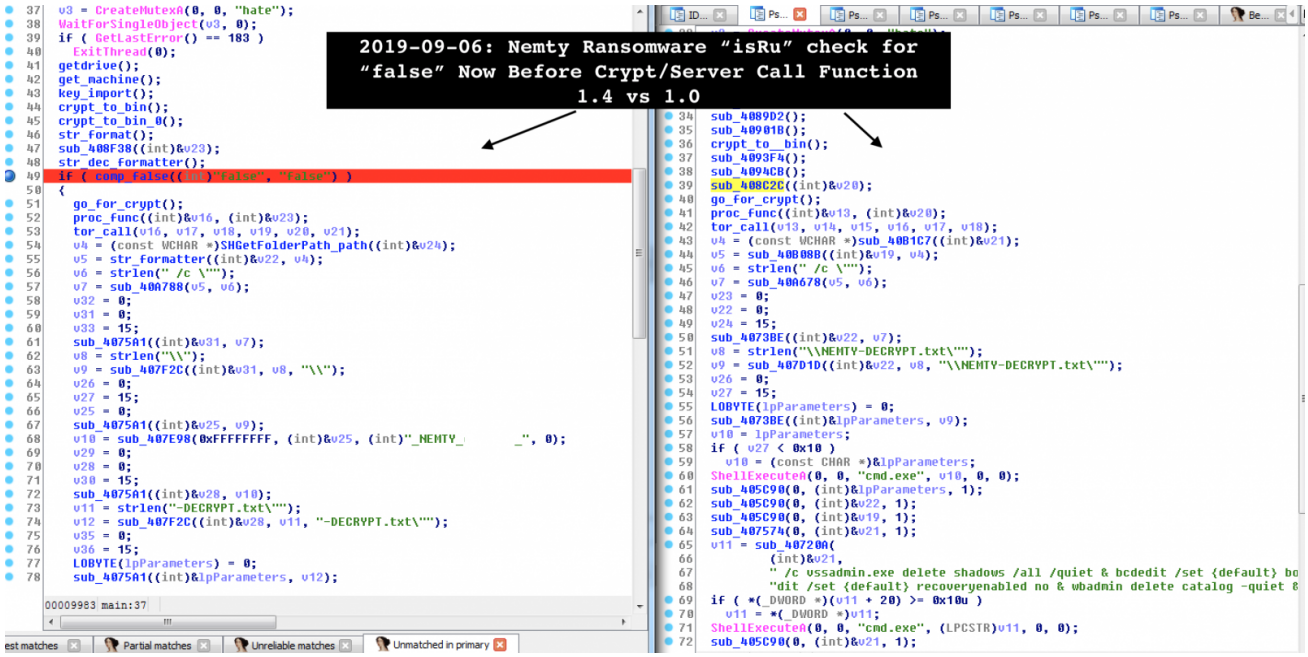
At a first look, the web page seems genuine as cybercriminals used visuals and the structure present on the original page.

To add to the deception, the cybercriminals also use what is known as homograph domain name spoofing for links to various sections of the site (Help & Contact, Fees, Security, Apps, and Shop).

The crooks achieved this by using in the domain name Unicode characters from different alphabets. To distinguish between them, browsers automatically translate them into Punycode. In this case, what in Unicode looks like paypal.com translates to 'xn--ayal-f6dc.com' in Punycode.

Security researcher Vitali Kremez analyzing this variant of Nemty ransomware noted that it is now at version 1.4, which comes with minor bug fixes.

One thing the researcher observed is that the "isRU" check, which verifies if the infected computer is in Russia, Belarus, Kazakhstan, Tajikistan, or Ukraine, has been modified. In the latest version, if the result of the check is positive, the malware does not move with the file-encrypting function, the researcher told BleepingComputer.



credit: Vitali Kremez

Computers outside these countries, though, are a target and will have their files encrypted and their shadow copies deleted.

Nemty ransomware has been present on cybercriminal forums for some time but it emerged on the radar of the infosec community towards the end of August, when security researcher Vitali Kremez published details of his analysis. The expert noticed in the code messages and references that made the malware stand out.

BleepingComputer tests showed that the ransom demand was 0.09981 BTC, which is about $1,000, and that the payment portal is hosted in the Tor network for anonymity.

At the end of August, another security researcher, Mol69, saw Nemty being distributed via RIG EK, which is probably an odd choice considering that exploit kits are on the brink of extinction as they target products that are on their death bed: Internet Explorer, Flash Player.

According to Yelisey Boguslavskiy of Advanced Intelligence, Nemty was received with "with extreme skepticism and aggression" on a cybercriminal forum, which is normal in that community. This may also influence its success, which is nothing compared to what Sodinokibi ransomware currently enjoys.

Update [09/08/2019, 18:00 EST]: Article updated with new information from security researcher Vitali Kremez.

Related Articles:

New Bumblebee malware replaces Conti's BazarLoader in cyberattacks

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Intuit warns of QuickBooks phishing threatening to suspend accounts

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

- Nemty Ransomware
- PayPal
- Phishing
- Ransomware

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

You may also like: