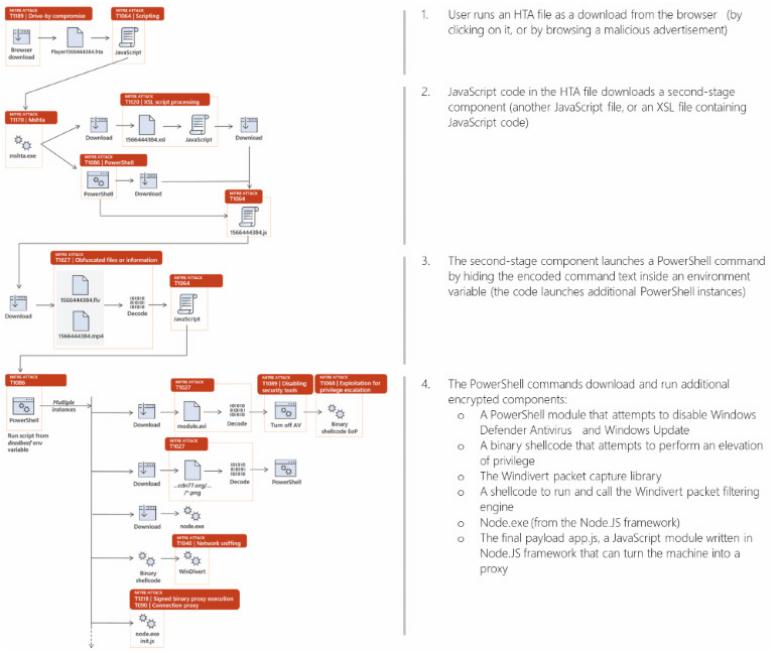
New malware using web application has turned into a source of attack, very difficult to detect

Recently, researchers from Talos (Microsoft) and Cisco have discovered a new type of malicious code that is very complex and has an extremely fast spreading speed.

Recently, researchers from Talos (Microsoft) and Cisco have discovered a new type of malware that is very complex and has an extremely fast spreading speed, has infected thousands of computer devices in Europe and America. This malware was named Microsoft Nodersok and Cisco Talos called Divergent.

This type of malware has a very complex mechanism of operation, it turns your computer into a bridge to continue access to the network (Proxy), then transfer to other devices.

Because the new malware has a fast spreading mechanism, hackers only need to create click-frauds, when a user clicks on it and transmits it to other devices via a computer network. Microsoft said hackers could use this malware to launch attacks on enterprise computer systems.



Describe the attack method of Nodersok malware. Photo: Microsoft.

Currently, there is no way to prevent this type of malicious code.

In early August, Windows Defender, Microsoft's antivirus detection software, was rated as one of the best anti-virus software by security researchers at the German AV-TEST Institute. However, according to Microsoft, Windows Defender can currently identify and block Nodersok, but it is difficult to determine which device is distributed.

Therefore, Microsoft encourages users to stay alert to unknown data and avoid launching HTA files in the computer system.

1. Beware of deceptive and spreading malicious code via notification links of Google Alert
2. Sim vulnerabilities threaten more than 1 billion phones globally