The unpatched Microsoft Word DDE vulnerability is exploited in a massive malware attack

A new attack method that exploits the Microsoft Office integration feature has been discovered being used for malware distribution campaigns.

A new attack method that exploits the Microsoft Office integration feature has been discovered being used for malware distribution campaigns.

Quantrimang reported on the Microsoft Office feature called Dynamic Data Exchange (DDE) that allows malicious code execution without the need to turn on Macros or affect memory. This is the protocol that Microsoft uses to allow 2 applications to share the same data, used on MS Excel, MS Word, Quattro Pro and Visual Basic to share data once and continue to exchange when updating .

See also: Features available on MS Office allow malware to enter without turning on the macro

Exploiting with DDE will not show warnings to users but only ask if they want to execute the application, and even this popup can be syntactically modified.

As soon as details of the DDE attack technique were announced, Cisco's Talos research group reported an attack campaign using this technique aimed at several organizations with in-house remote access Trojan names. DNSMessenger.

Necurs Botnets use DDE attacks to distribute ransomware

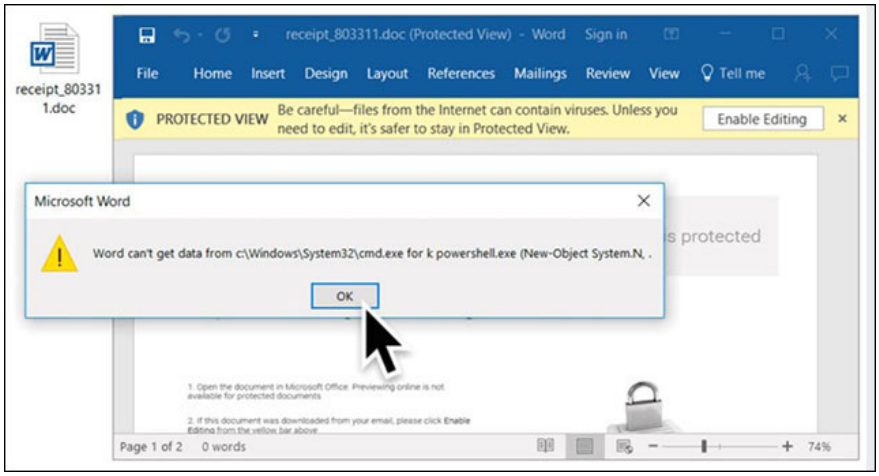
According to the SANS ISC, Necurs Botnet - malware currently controls more than 6 million infected computers worldwide and sends millions of emails - used to distribute ransomware Locky and TrickBot banking trojans, using Word files and exploiting them thoroughly. DDE art.

Locky had previously used macro traps on MS Office files but now updated Nercus Botnet to spread malware over DDE and hijack victims' screen shots.

'Downloader now has the ability to collect the victim's parameters. It captures the screen shot and sends it to the server, and details the error when the downloader fails. '

Malware Hancitor uses DDE attack techniques

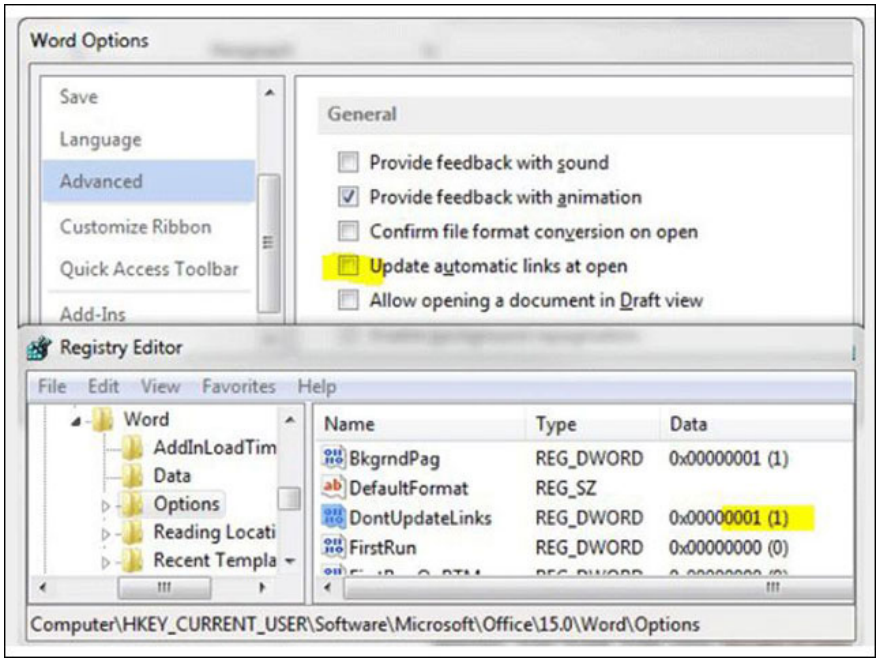
Another malware spam campaign was discovered as Hancitor (aka Chanitor and Tordal) using MS Office's DDE. This is a downloader that installs malicious payloads such as bank trojans, malware and ransomware onto infected machines and is often sent as MS Office files using macros in phishing emails.



Malware exploits attack techniques via DDE

How to protect yourself from DDE attacks?

Because DDE is a legitimate feature of Microsoft, most anti-virus software will not warn or block MS Office files and no one can give a patch.



Un-automatically update on Options

You can protect yourself by disabling the option to 'auto-update links when opening' on Office in **Word** > **Select File** > **Options** > **Advanced** and navigate to the **General** section **,** uncheck **'Update Automatic Links at Open'.**

See also: Google: Dangerous for users when Microsoft does not patch Windows the same way on the OS