BIZ & IT —

New Microsoft Word attacks infect PCs *sans* macros

Microsoft tells customers how to spot and block attacks.

DAN GOODIN - 11/11/2017, 6:30 AM

Microsoft

Enlarge

137

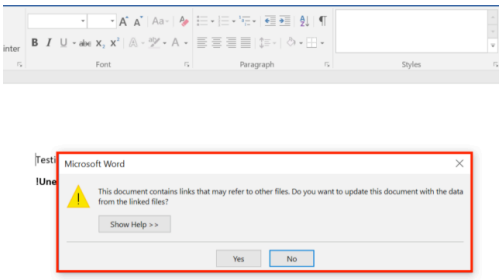
Fancy Bear, the advanced hacking group researchers say is tied to the Russian government, is actively exploiting a newly revived technique that gives attackers a stealthy means of infecting computers using Microsoft Office documents, security researchers said this week.

Fancy Bear is one of two Russian-sponsored hacking outfits researchers say breached Democratic National Committee networks ahead of last year's presidential election. The group was recently caught sending a Word document that abuses a feature known as Dynamic Data Exchange. DDE allows a file to execute code stored in another file and allows applications to send updates as new data becomes available.

In a blog post published Tuesday, Trend Micro researchers said Fancy Bear was sending a document titled IsisAttackInNewYork.docx that abused the DDE feature. Once opened, the file connects to a control server to download a first-stage of piece of malware called Seduploader and installs it on a target's computer. DDE's potential as an infection technique has been known for years, but a post published last month by security firm SensePost has revived interest in it. The post showed how DDE could be abused to install malware using Word files that went undetected by anti-virus programs.

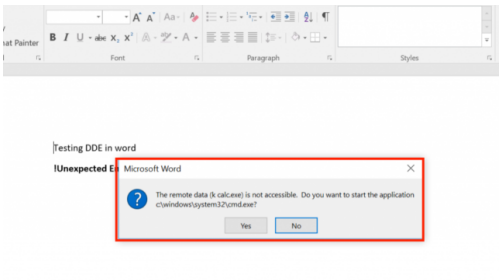
A day after Trend Micro published its report about Fancy Bear, Microsoft posted an

advisory explaining how Office users can protect themselves from such attacks. The easiest way to stay safe is to remain wary of unfamiliar messages that get displayed when opening a document. As SensePost first disclosed, before the DDE feature can be used, users will see a dialog box that looks something like the following:



Enlarge

If targets click yes, they will see a prompt that looks something like this:



SensePost

Enlarge

The malicious payload will only execute after a user has clicked yes to both warnings.

The Microsoft advisory also

explains how more technically advanced users can change settings in the Windows registry to disable automatic updating of data from one file to another.

Fancy Bear isn't the first group to actively exploit DDE in the wild. A few weeks after the SensePost post went live, researchers reported attackers were abusing the feature to install the Locky ransomware.

Many researchers have remarked on the ability of the DDE-enabled attacks to spread malware through Office documents without the macros. The novelty is likely to make DDE effective in some settings, given the growing awareness of the dangers macros pose. But ultimately, the DDE mechanism comes with its own telltale signs. People should learn to recognize them now that DDE attacks are growing more common.

DAN GOODIN

Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL
dan.goodin@arstechnica.com
// **TWITTER** @dangoodin001

READER COMMENTS 137 SHARE THIS STORY

← PREVIOUS STORY NEXT STORY →

Related Stories

Today on Ars

RSS FEEDS CONTACT US
VIEW MOBILE SITE STAFF
VISIT ARS TECHNICA ADVERTISE WITH US
UK REPRINTS
ABOUT US