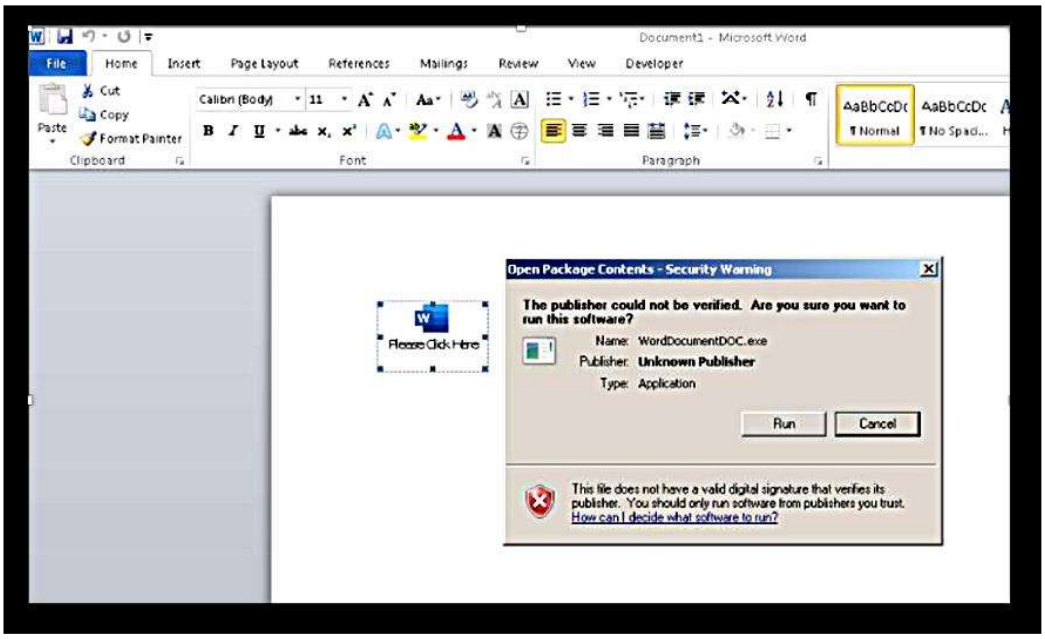
Microsoft Turns Macros Off Back On & Another Reason to Switch To Windows 11



Source: https://blog.reversinglabs.com/blog/smash-and-grab-astralocker-2-pushes-ransomware-direct-from-office-docs

On July 7, 2022, this blog posted an article on the topic of **Word Malware**. And how macros can look like one thing, but actually be something else. The example above shows a file that has DOC in its filename. The file name ends, however, with the suffix ".exe", notating that the file is actually an executable that, if we clicked on, will run some kind of application, usually an installer. And, because there is just no good gosh darn reason to download macro laden Office docs from the Internet, Microsoft intended to block macros from downloading from online sources completely. And, as abruptly as the change was announced, the original announcement was pulled back, but that announcement came from a blog posting of one MS Minion. One day later, in another blog posting another MS Minion rolled back the previously announced rollback of the previously proposed macro blocking.

Then on **July 20, 2022**, came a multitude of MS Minions in a mutual meeting of the minds, and made a mighty unambiguous statement that Macros from the internet will be blocked by default in Office. It's as if the Gnomes of Redmond channeled their best Ron Ziegler and declared, "**This is the operative statement. The others are inoperative**."

The Dispatch From the Front referenced above recommended turning off macros altogether, and not wait for MS to make up its mind. Macros are a thing of the past, like **web frames pages**. And the article offered, I like to think clear and relatively easy instructions on how to disable macros altogether. And, apparently, the Gnomes of Redmond agree. Microsoft's date for the disabling of macros from the Internet is to take affect July 27, 2022. Below is a link to a deep dive into Microsoft's reasoning for blocking macros, a 25 page paper, with the boffo title: "**Macros from the internet will be blocked by default in Office.**" MS made the paper easily available, and a **pdf is available here**.

> **Even before this change we're introducing, organizations could use the Block macros from running in Office files from the Internet policy to prevent users from inadvertently opening files from the internet that contain macros. We recommend enabling this policy as part of the security baseline for Microsoft 365 Apps for enterprise. If you do configure the policy, your organization won't be affected by this default change.**

I do not think that this change in policy will affect too any users that are not part of a larger enterprise. I still use an Access database as my own general ledger I wrote myself in 2001 that is powered by VBA macros. But I wrote it! It did not originate from or go out onto the Internet. If, however, you are a member of a larger group that has been using Office for many years, and concerned about this change causing you disruptions, Microsoft has made available a tool to help locate macro enabled Office files on your network. I offer the text below only as a public service.

> **To identify files that might be impacted by using the Readiness Toolkit, follow these basic steps:**
>
> **1. Download the most current version of the Readiness Toolkit from the Microsoft Download Center. Make sure you're using at least Version 1.2.22161, which was released on June 14, 2022.**
>
> **2. Install the Readiness Toolkit.**
>
> **3. From a command prompt, go to the folder where you installed the Readiness Toolkit and run the ReadinessReportCreator.exe command with the blockinternetscan option.**

So, *If that's your idea of a good time,* to quote Julius, that great Marxist philosopher.

It has been speculated in these pages for some time now that some kind of intervention by a power greater than us mere users will arise simply because the gravity of the situation is pulling down the Internet like gravity. Phishing emails, smishing SMS texts, poison websites are all ways of attack to some degree within the control of the enlightened computer users. Simply do not respond. Wash and repeat as needed. Other common forms of attacks are,

however, more subtle. One such form of a stealthy attack is a brute force attack. At its most basic, in a brute force attack a hacker will simply keep trying to guess the password to gain system access. As **CloudFlare defined a brute force attack**:

> **A brute force attack is a trial-and-error method used to decode sensitive data. The most common applications for brute force attacks are cracking passwords and cracking encryption keys.**

In May 2022, brute attacks on Windows Servers in the State of Maryland rose by 78%. Over a 14 day period, "**automated hacking attempts soared by 78 percent. That means 1,100 total the sum total of brute-force attacks in the Maryland in the course of the 14 days prior**," reported security vendor **Syspeace, May 30, 2022**. In the same report, "**brute-force attacks in Illinois and Minnesota have grown. With 380 blocked automated hacking attempts per Syspeace-secured server the two weeks prior, Illinois has witnessed a growth of 230 percent in comparison with the previous 14 days. In Minnesota, the amount has risen by 41 percent to 56 automated hacking attempts per Windows server secured by Syspeace.**"

Of course, there are several tools on the web to automate the process of what is essentially password guessing. One such tool, **"the THC-Hydra tool**," is used by security analysts "**to identify vulnerabilities in client systems.**"

> **Hydra quickly runs through a large number of password combinations, either simple brute force or dictionary-based. It can attack more than 50 protocols and multiple operating systems. Hydra is an open platform; the security community and attackers constantly develop new modules.**

For a hacker to gain the chance to crack a password remotely, the hacker must first gain access to the device itself. In the Windows world, that remote access is often accomplished by exploiting vulnerabilities in the Windows Remote Desktop Protocol (RDP). Since 2020, "**RDP is regarded as the single biggest attack vector for ransomware," cyber-security firm Emsisoft said last month, as part of a guide on securing RDP endpoints against ransomware gangs.** "

One method of thwarting brute force password cracking attacks is to limit the number of failed logon attempts before a lockout occurs. This is known as "**rate limiting.**"

> **Rate limiting works by throttling the speed at which attackers can make password guesses, typically by shutting them out for a period of time after a small number of incorrect guesses. This is mildly inconvenient to a real user who is unlikely to make more than a handful of incorrect guesses before calling support, but represents a huge barrier for a computer program looking to race through tens or even hundreds of thousands of password attempts.**

Microsoft now intends to automate the rate limiting procedures in Windows 11.

> **Microsoft is rolling out a new security default for Windows 11 that will go a long way to preventing ransomware attacks that begin with password-guessing attacks and compromised credentials. The new account security default on account credentials should help thwart ransomware attacks that are initiated after using compromised credentials or brute-force password attacks to access remote desktop protocol (RDP) endpoints, which are often exposed on the internet.**

The purpose is to limit by default the number of failed logon attempts and then implement a system lockout. The feature is currently only available to the Windows 11 Insider Preview. But Microsoft is using the Insider Preview to test new features, as MS readies the Windows 11 22H2 update due out soon.

I am not the only long time Windows user who views the two changes noted herein as very good news. **As one UK Windows security expert tweeted**:

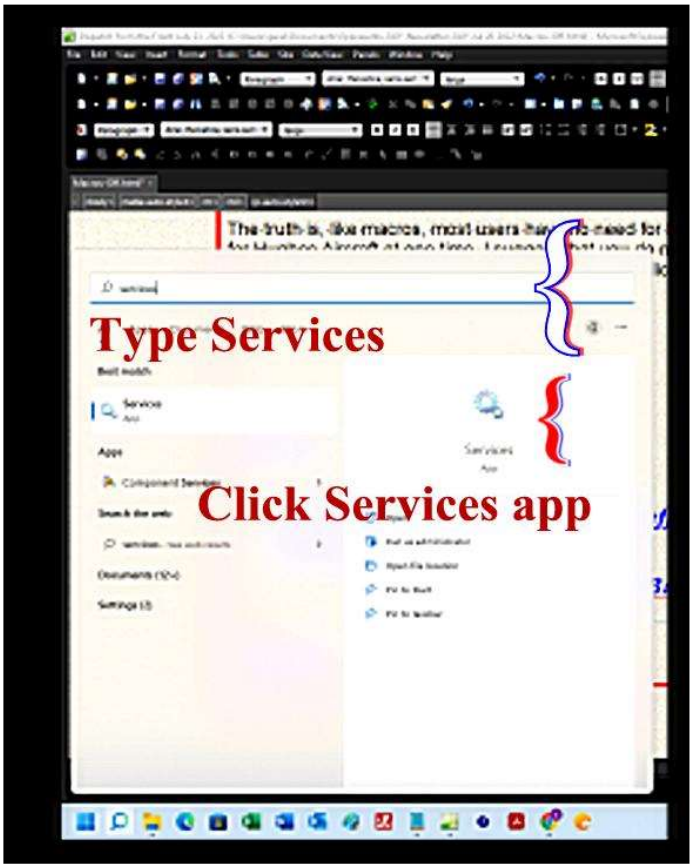
> **oh my god, they're doing the RDP entry issue - between macros and RDP this makes almost all Windows/MS ransomware entry.**

I didn't say that. He did.

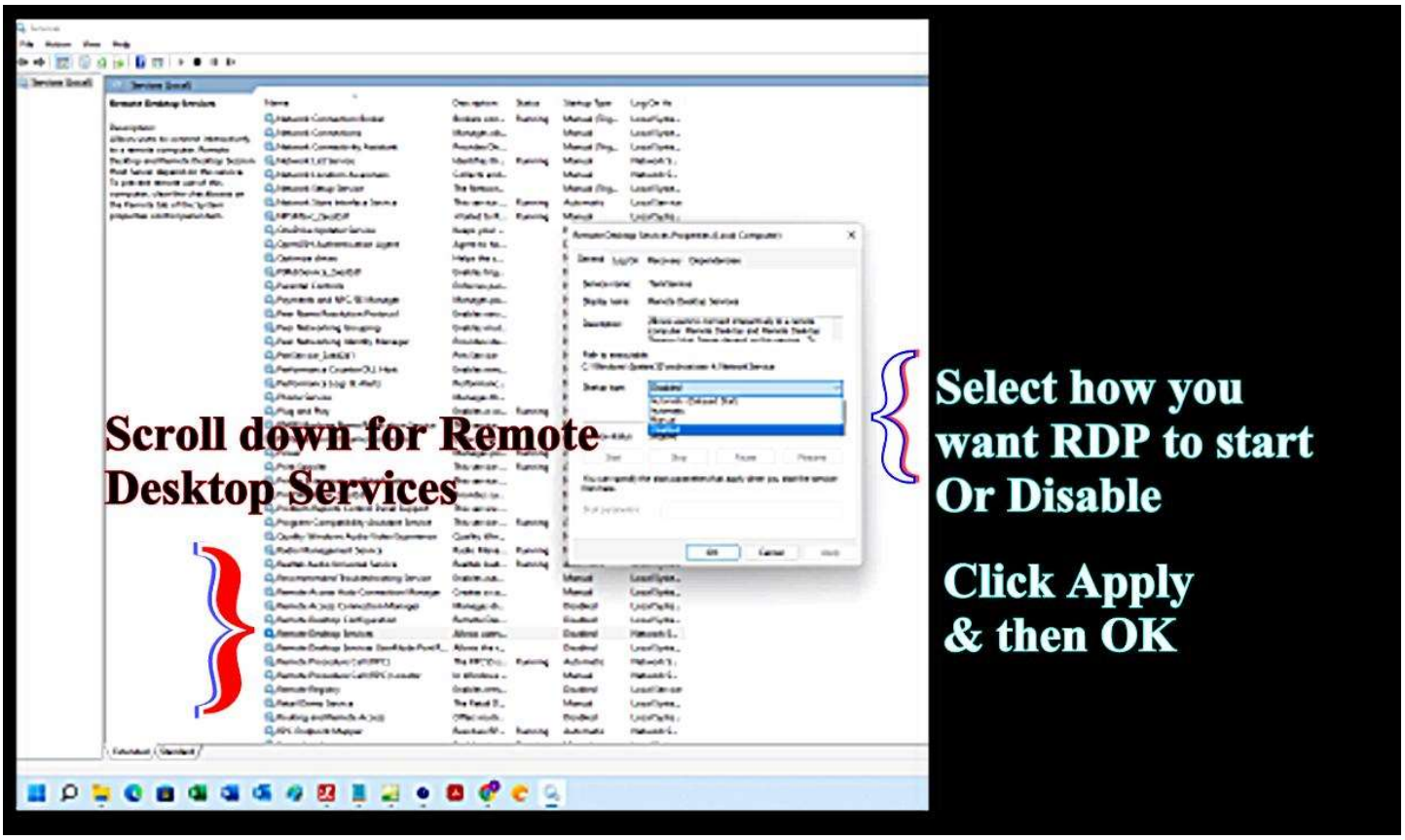
I would argue that, like macros, most users do not need Remote Desktop Protocol enabled by default. Maybe your Uncle Ernie did work for Hughes Aircraft at one time; I would nevertheless not let him access you computer remotely for his tech help. A legitimate and professional tech support firm will have its own remote access app.

To access the RDP control to enable/disable RDP we must first open the SERVICES app.

1. Click into the searchbar and type "services." Then click on the services app.



2. Click the Services app. Scroll down and locate "Remote Desktop Services." Start/Stop — Disable/Enable as is your choice.



And that's all you need to do to shut off and out those who want into your PC.

Note: Pay Attention that you only disable Remote Desktop Services.

Keep a knockin', but you can't come in.
Keep a knockin', but you can't come in.
Keep a knockin', but you can't come in,
Come back tomorrow night and try again.

— Keep A-Knockin', Richard Penniman (Little Richard)

Back to Top

Gerald Reiff

Back to Top ← previous post next post →