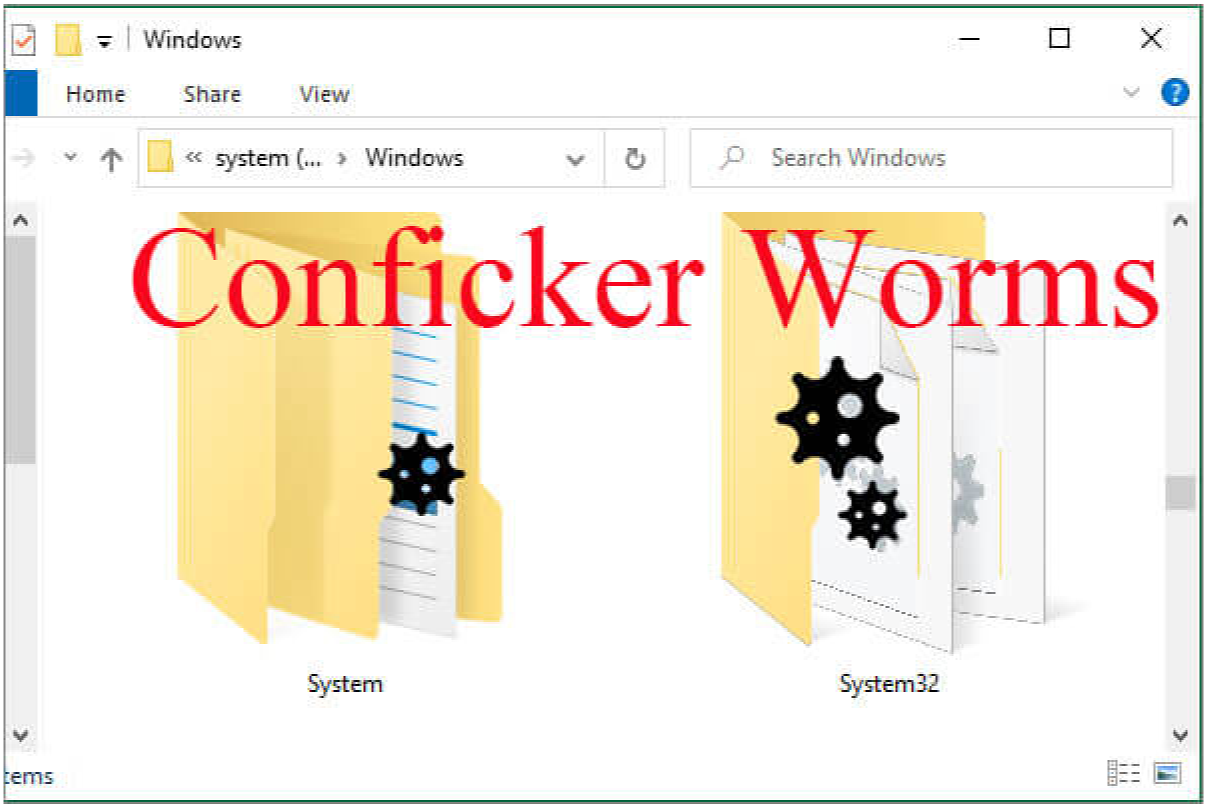
Conficker - One of the Most Prevalent & Complex Windows Worms [MiniTool Tips]

minitool.com/backup-tips/conficker-worm.html

Helen

March 12, 2021

Summary :



This article written by MiniTool Tech reviews one of the world's most infectious and sophisticated computer viruses – Conficker. It elaborates on its definition, history, impact, propagation mechanism, as well as the way to avoid being infected with Conficker, almost everything you want to know about the malware (Wiki -level)!

What Is Conficker?

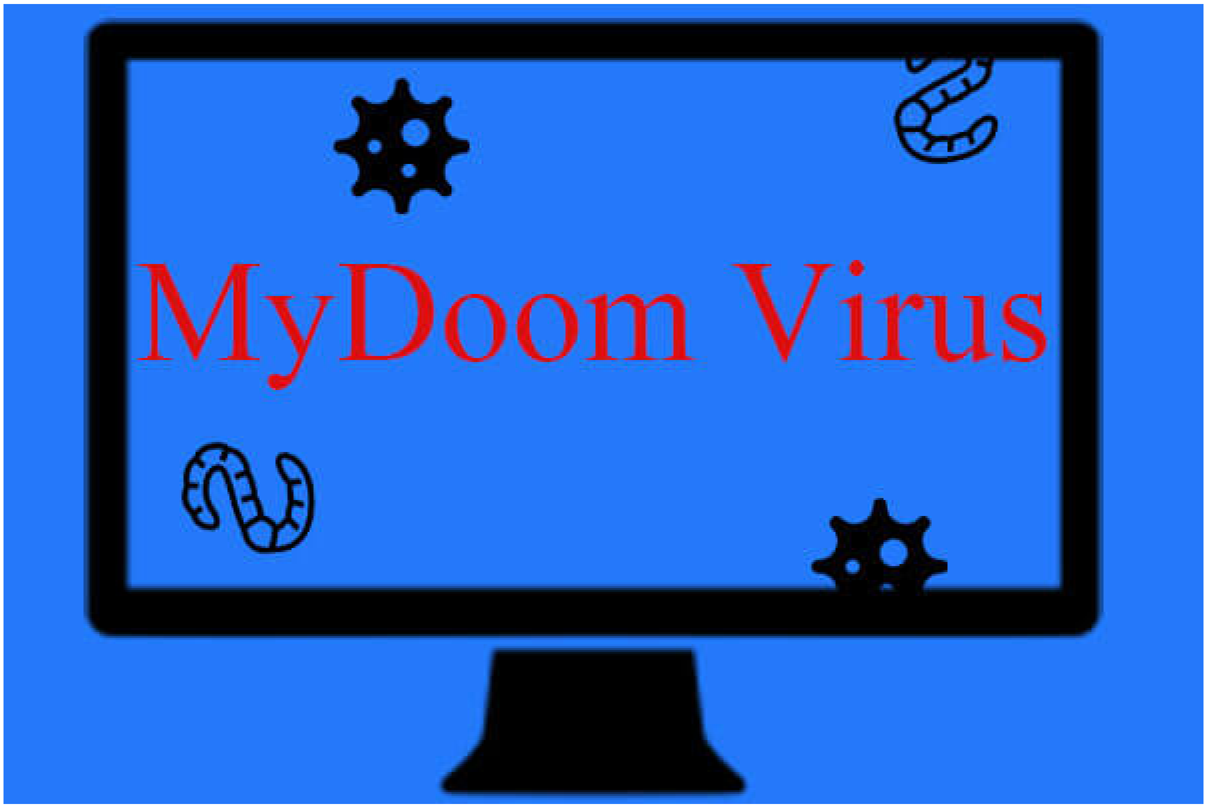
Conficker, also called Downadup, Downup, or Kido, is a kind of computer virus attacking the Windows operating system (OS). It makes use of vulnerabilities of system programs and dictionary attacks on administrator passwords to spread while forming a botnet.

It is usually difficult to counter victims for Conficker uses multiple advanced virus technologies. **Conficker worms** attacked millions of computers including home personal PCs, business machines, and government devices in more than 190 countries. It becomes the largest known computer worm infection since Welchia in 2003. Conficker was first detected in November 2008.

Tip: Welchia, also called the “Nachi worm”, is a computer malware that exploits a flaw in the Microsoft remote procedure call (RPC) service.
Although Conficker propagated widely, it didn’t cause much damage. The reason is that maybe its designer didn’t dare to use it for the virus drew much attention worldwide. Conficker doesn’t destroy or steal data. The main purpose of it is to infect as many Windows computers as possible, which makes it the most infectious computer virus.

How Does “Conficker” Come From?

The name of the **Conficker virus** is said to be originated from the English word “configure” and the German word “ficker” (means “fucker” in English). However, Joshua Phillips, a Microsoft analyst, offers another interpretation of the name “conficker”. Joshua states that “conficker” is a rearrangement of portions of the domain name trafficconverter.biz, which was used by early Conficker versions to download updates. The letter “k”, which isn’t found in the domain name, is added to avoid a “soft” c sound.



Impacts of Conficker

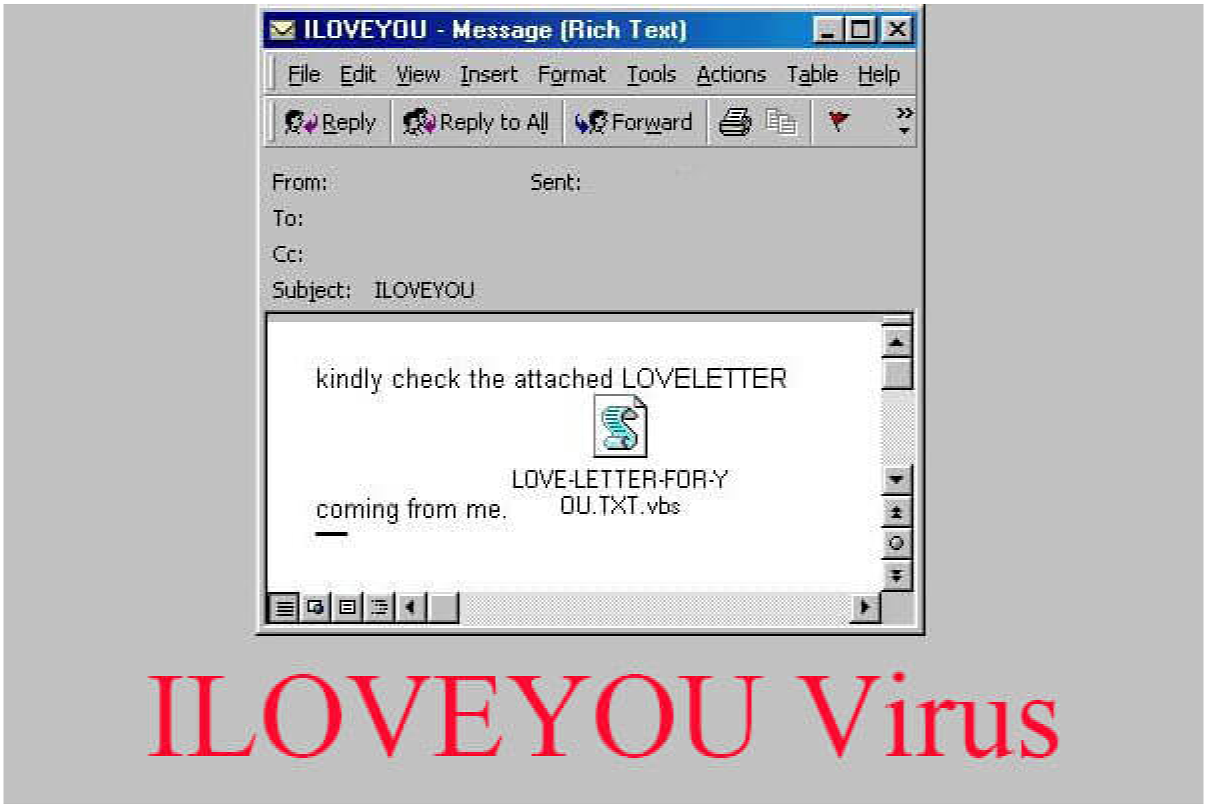
The British Ministry of Defence reported that some of its major systems and computers were infected. Conficker had spread across administrative offices, NavyStar/N* desktops on various Royal Navy submarines & warships. And, it was reported that over 800 machines were infected across the city of Sheffield.

Intramar, a French Navy computer network, was infected with Conficker on January 15, 2009. It was quarantined subsequently, which resulted in aircraft in several airbases being grounded for their flight plans couldn't be downloaded.

On February 2, 2009, the Bundeswehr, the unified armed forces of Germany, reported around 100 infected computers. In the same month, the infection of the IT system of Manchester caused about 1.5 million pounds of financial loss. A USB flash drive was believed to be the initial source of Conficker, so the usage of USB was banned then.

On March 24, 2009, the memo of the UK Parliamentary ICT service informed the users of the House of Commons that it (the service) had been infected with Conficker. The memo was from the director of the service and was leaked subsequently. It called for users to avoid connecting any unauthorized equipment to the network.

In January 2010, the Greater Manchester Police computer network was infected. This caused the police computer network to be disconnected from the Police National Computer for 3 days, as a precautionary action. During the three days, police officers had to ask other forces to run routine checks on people and vehicles.


ILOVEYOU - Message (Rich Text)
File Edit View Insert Format Tools Actions Table Help
Reply
Reply to All
Forward
ILOVEYOU Virus

From:
Sent:
To:
Cc:
Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.

LOVE-LETTER-FOR-YOU.TXT.vbs

[Review] What Is the ILOVEYOU Virus & Tips to Avoid Virus
What's ILOVEYOU virus? What did it do? When did it start and how did it stop? Who created it and in what language was it created? Find all answers here!

Read More

What Does the Conficker Virus Do?

Though almost all of the advanced virus technologies adopted by Conficker have been seen in past viruses and are well known to researchers, the combination of so many made Conficker extremely difficult to clear. Also, the developers of Conficker were tracking anti-virus actions from network operators. Thus, they released new versions to patch the malware's own flaws.

There were 5 variants of Conficker and they are named Conficker A, Conficker B, Conficker C, Conficker D, and Conficker E. Those five versions were first detected respectively on November 21, 2008; December 29, 2008; February 20, 2009; March 4, 2009; and April 7, 2009.

The **Conficker working group** uses namings of A, B, B++, C, and E for the same version respectively. That is to say, (MSFT) C is equivalent to (CWG) B++ and (MSFT) D is equivalent to (CWG) C. The names used in this article are based on the MSFT (Microsoft).

Conficker Infection

Version A, B, C, and E use MS08-067 flaw in Server service (NetBIOS), in which an already-infected source machine uses a specially-crafted RPC request to force a buffer overflow and execute shellcode on the target computer.

On the source computer, Conficker malware runs an HTTP (Hypertext Transfer Protocol) server on a port between 10000 and 1024. The target shellcode connects back to the HTTP server to download a copy of the malware in DLL form, which then attaches to svchost.exe. Conficker B and later may also attach to a running Windows Explorer process. Yet, attaching to those processes might be discovered by the trust feature of an installed firewall.

Windows Utility Used by Malware! It Is a Big Problem!

Windows utility used by malware? It is true. To know more information about this situation, you can read this post.

Read More

While Variant B and C also make use of removable media by creating DLL-based AutoRun trojan on attached removable devices for propagation. They can remotely execute copies of themselves via the administrative share on computers visible over NetBIOS. If the share is protected by a password, a dictionary attack is attempted, potentially generating large amounts of network traffic and tripping user account lockout policies.

B and C variants place a copy of their DLL form in the recycle bin of any attached removable drives, from which they can then infect new hosts via the Windows AutoRun mechanism using a manipulated autorun.inf.

To start itself at system boot, Conficker saves a copy of its DLL form to a random filename in the Windows system or system32 folder and adds registry keys to let svchost.exe invoke that DLL as an invisible network service.

Tip: Conficker is also known as win32 Conficker.

Conficker Propagation

Conficker has a few mechanisms to pull or push executable payloads over the network. Those payloads are used by Conficker to update itself to newer versions and install additional viruses.

Version A generates a list of 250 domain names each day across 5 TLDs (Top-Level Domain). The domain names are generated from a PRNG (Pseudo-Random Number Generator) seeded with the current date to ensure that each copy of the worm generates the same names every day. Then, Conficker attempts an HTTP connection to each domain name in turn, expecting from any of them a signed payload.

While, Version B increases the number of TLDs to 8 and has a generator tweaked to produce domain names different from those of A. To counter Conficker's usage of pseudorandom domain names, ICANN (Internet Corporation for Assigned Names and Numbers) and some TLD registries began a coordinated barring of transfers and registrations for those domains in February 2009.

While, Version D counters pseudorandom domain names by generating daily a pool of 50 thousand domains across 110 TLDs, from which it randomly selects 500 to attempt for that day. The generated domain names were also shortened from 8 – 11 to 4 – 9 characters to make them more difficult to detect with heuristics.

The Different Types of Malware and Useful Tips to Avoid Them
Malware is one of the biggest threats on the Internet. This post provides information about different types of malware and you can know how to avoid them.

Read More

The new pull mechanism is unlikely to spread payloads to more than 1% of infected computers each day. Yet, it is expected to function as a seeding mechanism for Conficker's peer-to-peer (P2P) network. The shortened generated names are expected to collide with

150 – 200 existing domains each day, potentially resulting in a DDoS (Distributed Denial-of-service) attack on websites serving those domains. Yet, the large number of generated domains and the fact that not every domain will be contacted for a given day will probably prevent DDoS situations.

B, C, and E versions perform in-memory patches to NetBIOS-related DLLs to close MS08-067 and open reinfection backdoor in Server service via the same flaw. Variant C also creates a named pipe, over which it can push URLs for downloadable payloads to other infected computers on a LAN.

Besides, Variant D and Variant E also use a custom protocol to scan for infected peers via UDP (peer-to-peer mechanism) and then transfer via TCP.

Conficker Self-Defense

Besides the wonderful infection and propagation mechanisms, Conficker also has advanced self-protecting systems. Its Version B, C, D, and E can block certain DNS lookups and disable AutoUpdate. Especially, Variant D does an in-memory patch of DNSAPI.DLL to block lookups of anti-malware-related sites.

[Answered] Is Vimm's Lair Safe? How to Use Vimm's Lair Safely?
Is Vimm's Lair safe to use and download old video game ROMs, emulators, or manuals? What websites are Vimm.net alternatives? How to keep safe while using Vimm?

Read More

Version D of Conficker also disables Safe Mode. Together with version E, version D also kills anti-malware by scanning for and terminating processes with names of anti-malware, patch, or diagnostic tools at one-second intervals.

Moreover, each version of Conficker ends up updating itself to the next version or higher versions. Especially, the final version of Conficker, version E, also downloads and installs malware payload, Waledac spambot and SpyProtect 2009 scareware.

Conficker Today

Though it has been over ten years since Conficker appeared and Conficker has dropped out of people's attention, every year, there are still thousands of computers infected by it. Though Conficker won't cause data loss to victims, it does increase the network payload of them greatly. Thus, the infected computers will experience slow network performance and it will influence the usage of them.

How to Avoid Conficker?

1. Update Windows
2. Scan for USB and shares
3. Disable AutoRun and AutoPlay
4. Enable firewall and antivirus

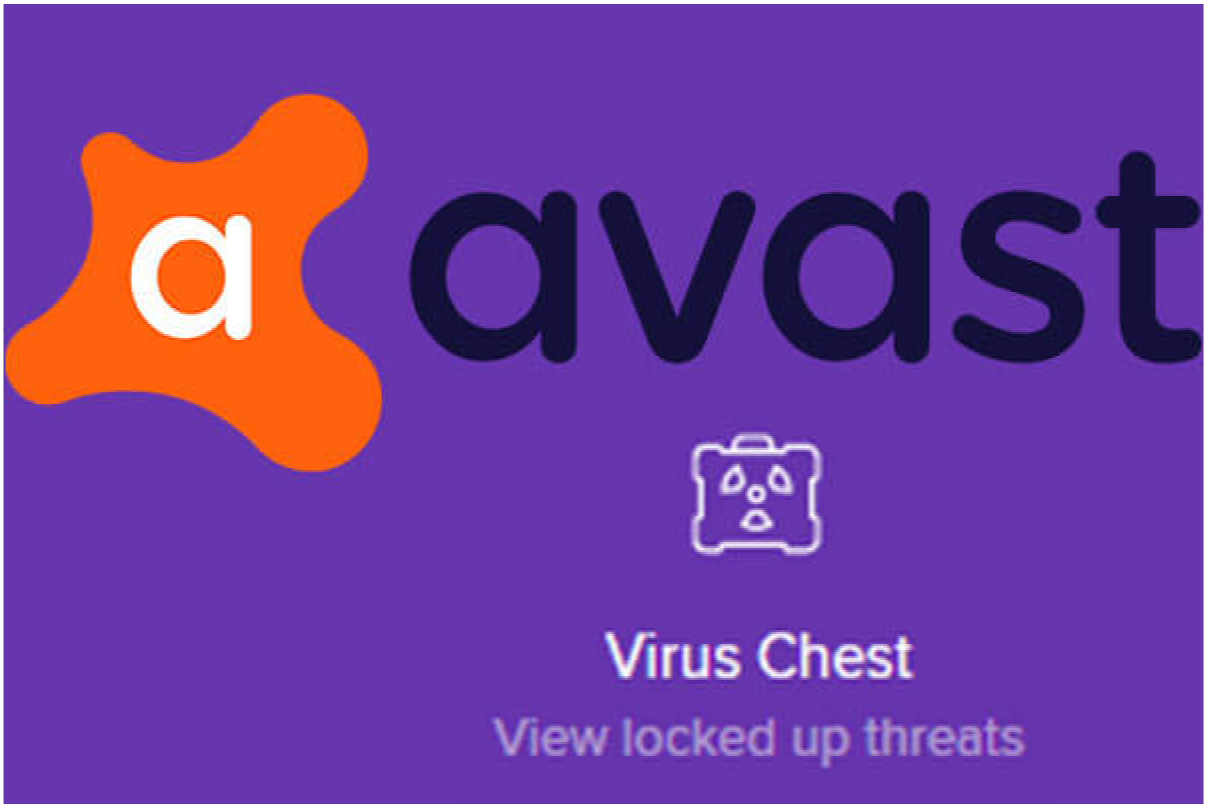
How to Avoid Being Infected with Conficker?

Since Conficker still brings inconvenience to you if your computer is infected by it, you'd better not get attacked by it. Then, how to protect yourself from being infected by Conficker? Below suggestions are listed for your reference.

#1 Get Your System Patched Immediately

If you are still using an old OS that is vulnerable to virus Conficker, the most urgent thing is to update Windows better to its newest version. Therefore, you have shut down the backdoor for the malware.

How to determine whether your system is vulnerable to Conficker or not? Generally, if you are using Windows 7 or later edition, you are safe from Conficker. If you are running a system earlier than Windows 7, especially with MS08-067 network service, you are probably to be infected by Conficker. Just update your OS will solve the problem!



Secure Computer by Avast Virus Chest & MiniTool ShadowMaker
What’s Avast Virus Chest? How to check/view Avast Virus Chest? How to restore files from Avast Virus Chest? How to delete a file from Avast Virus Chest?

Read More

#2 Be Careful When Connect to USB or Open Shared Files

Since one of the spreading ways of Conficker is through USB flash media or shares, you are strongly recommended to pay attention to the removable devices you are going to connected to your computer and shared files (you received) you are going to open, especially the unauthorized devices and shares from strangers.

What should you do? Never use a USB or open a shared file? No! You can still use USB and shares since they are unavoidable nowadays. The thing you need to do is to take a security scan on the target USB drive or share with **Conficker detection tool**, **Conficker removal tool**, or **Conficker scanner** like Sophos Intercept X Endpoint.

#3 Turn off Autorun for USB

Some of you may argue that once you insert a removable drive into your computer, it will be opened automatically without your permission. Thus, you don’t have a chance to scan it for viruses. In such a situation, you should turn off the autorun service of your system for external media like USB.

When you successfully disable the AutoRun or AutoPaly functionality, next time when you connect a USB to the machine, it will ask you before open and run it on the host.

#4 Monitor OS with Firewall and Antivirus

Protecting your computer from viruses, malware, worm, trojan, spyware, etc. is a lifetime task. No one can do it manually or alone. Therefore, it is recommended to rely on a firewall and antimalware to give complete and continuous protection to your computer.

There are also some other methods to prevent yourself from Conficker like setting a strong network password, applying a device control policy…

Click to tweet

How to Prepare Yourself for Future Infection?

As far as this article was written, no version of Conficker causes data loss to its infected computers. Yet, no one can guarantee that there is also no data loss caused by Conficker. It may update itself and start to destroy victims' files in the future as most modern computer malware do. If so, what can we do for the preparation of the possible damage?

Our purpose is to avoid losing data. If we can't avoid being infected by Conficker or other viruses for 100%, then, we can at least create more copies of our important files and save them in various places. Thus, even if one or two locations are attacked, we can still have the rest and keep our normal work. Then, how to quickly make copies of files in a reasonable manner?

Usually, if you want to back up crucial files in a reasonable way, you'd better ask for help from professional and reliable software, such as MiniTool ShadowMaker. It is specially designed for backing up and restoring files, systems, hard disks, partitions/volumes, and so on. Let's see how it works.

Step 1. Download and install MiniTool ShadowMaker on your computer.

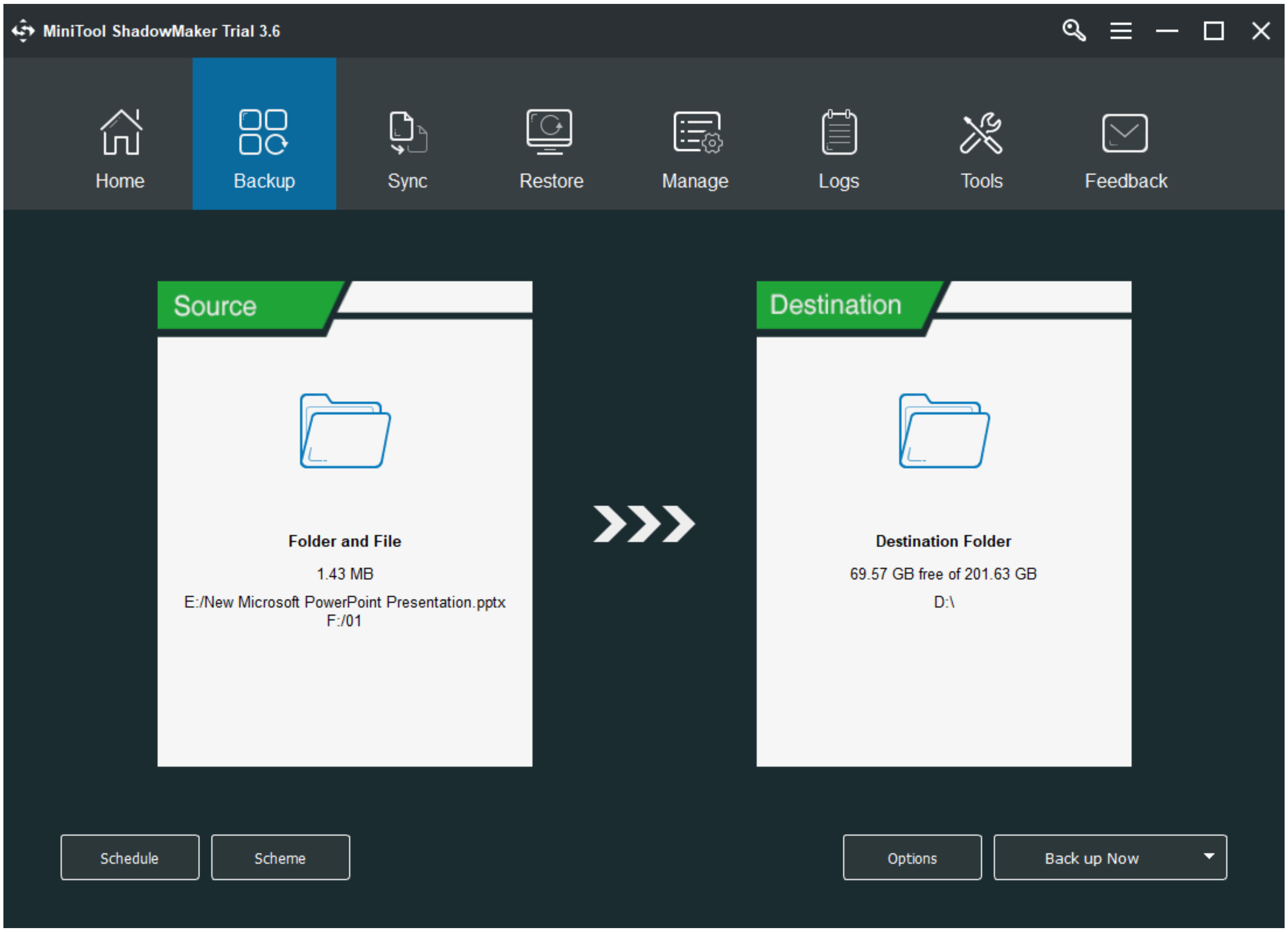
Free Download

Step 2. Launch the program and click **Keep Trial** to try its wonderful features.

Step 3. In its main interface, click **Backup** in the upper menu.

Step 4. In the Backup screen, click the **Source** module to select the items you plan to back up on your machine.

Step 5. Then, click the **Destination** module to specify where to save the backup image. External storage place is recommended. Also, note that the target storage location will be overwritten.



Source

Folder and File

1.43 MB

E:/New Microsoft PowerPoint Presentation.pptx
F:/01

Destination

Destination Folder

69.57 GB free of 201.63 GB

D:\

Step 6. Check the backup task. If you'd like to back up those source files regularly, just set a scheduled backup for them by clicking the **Schedule** button. Finally, confirm the task by clicking the **Back up Now** button in the lower right.

The backup task will start after another confirmation. Then, just wait for the success of the procedure. Once finished, just exit the application.

Ok, the above is all about the Conficker worm I'd like to share in this article. If you want to read more related information, just search on this website. If you have anything about Conficker to discuss, just use the below comment section. Or, if you encounter any problem while using MiniTool ShadowMaker, feel free to contact [email protected].