

What is the PowerSniff malware? - The Security Buddy

By Amrita Mitra

Published: 2017-03-09 · Archived: 2026-04-05 19:56:45 UTC

What is the PowerSniff malware?

PowerSniff is a malware program that is distributed to victims via spam emails with a Microsoft Word Document attachment. It uses some [social engineering techniques](#) to convince a victim to click on the attachment. When the victim clicks on the Microsoft Word Document attachment, a malicious macro embedded in the file starts executing. The malicious macro infects the computer with malware.

How does the PowerSniff malware infect a computer?

At first, a victim gets an email with a Microsoft Word Document attachment. The majority of the emails contain specific information about the victim's company, like its physical address, phone number, etc. As a result, the victim gets deceived easily, and the possibility that the victim will click on the attachment increases.

When the victim clicks on the Microsoft Word Document, a malicious macro contained in the file starts executing. A Microsoft Word Document macro is a series of commands and instructions that can be grouped together as a single command to accomplish a specific task automatically.

This macro invokes the WMI service, which executes a hidden instance of powershell.exe. It checks whether the system is a 32-bit or a 64-bit machine. Based on that information, it downloads and executes another malicious file on the system.

The downloaded file is a PowerShell script, which contains a shell code and is subsequently decoded and executed. This shellcode decrypts and executes an embedded payload.

The malware then performs a number of actions to determine a few information, like whether the system is running in a sandbox or virtualized environment and some specific information about the victim. The malware mainly tries to determine whether the victim works in any financial institution or the device is actively used in financial transactions. The malware seems to avoid a machine that is a part of a healthcare or educational organization. And, if the conditions are met, the victim's machine is marked as interesting to the attackers.

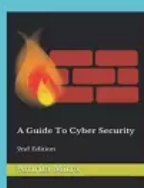
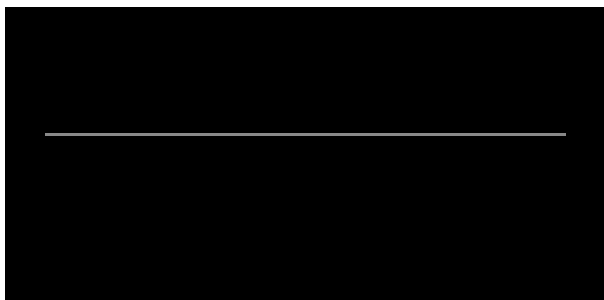
How to prevent the PowerSniff malware?

The following prevention mechanisms can be taken to safeguard a user from falling victim to this malware:

- As this malware relies on Microsoft Word Document macros, please ensure macros are not enabled in Word documents by default.
- If you are not very sure of the authenticity of the source, please avoid opening any macros contained in the file.

- Please avoid clicking on an email attachment if you are not sure about the sender of the email.

I hope this helps. Interested readers who want to know more about how different malware and cyberattacks work and how we can prevent them may want to refer to the book "[A Guide To Cyber Security.](#)"



A Guide To Cyber Security, 2nd Edition

Author: Amrita Mitra

The book explains how various malware and cyber attacks work and how we can prevent them. More ...



A Guide To Cyber Security, 2nd Edition

Author: Amrita Mitra

The book explains how various malware and cyber attacks work and how we can prevent them. More ...

Source: <https://www.thesecuritybuddy.com/malware-prevention/what-is-powersniff-malware/>