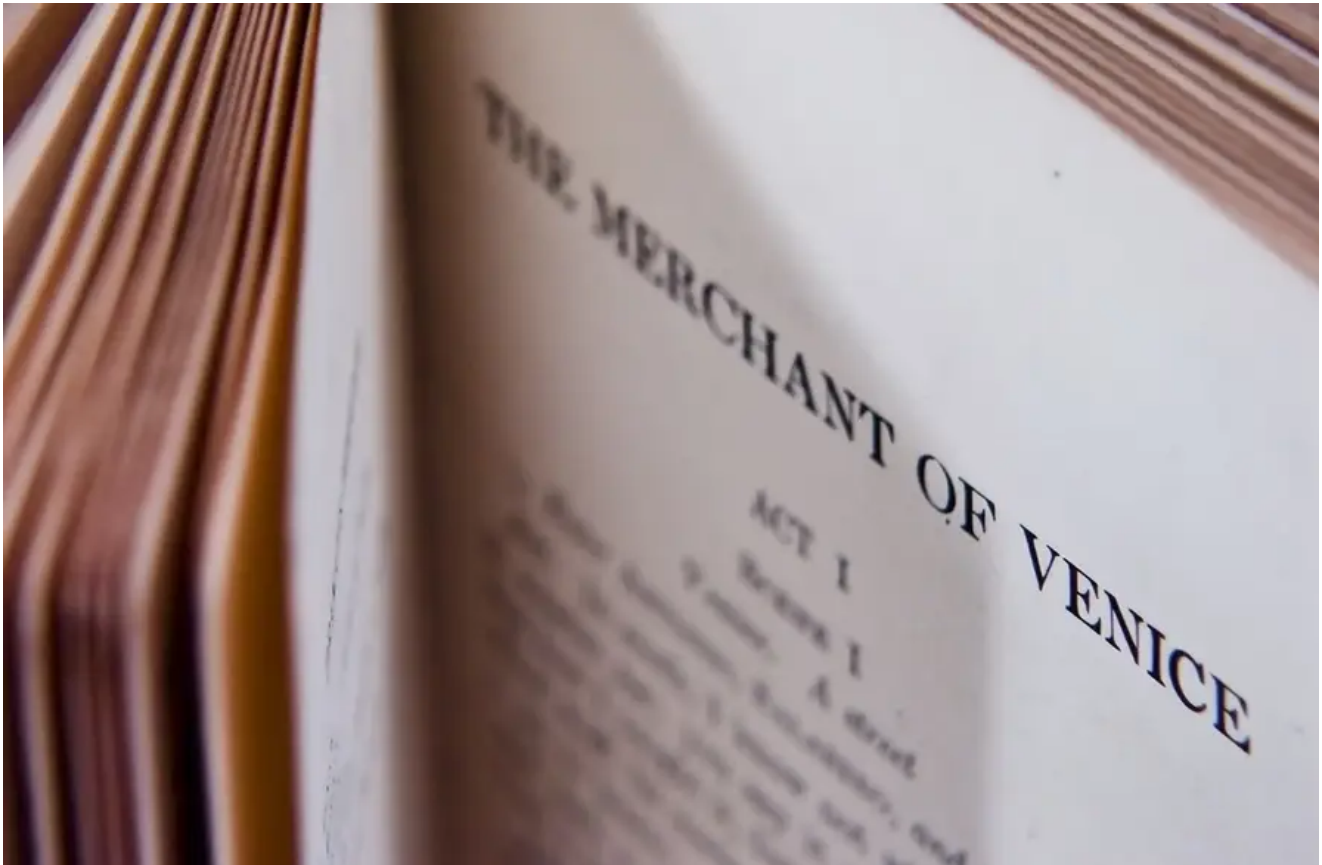


# Shylock Polymorphic Financial Malware Infections on the Rise

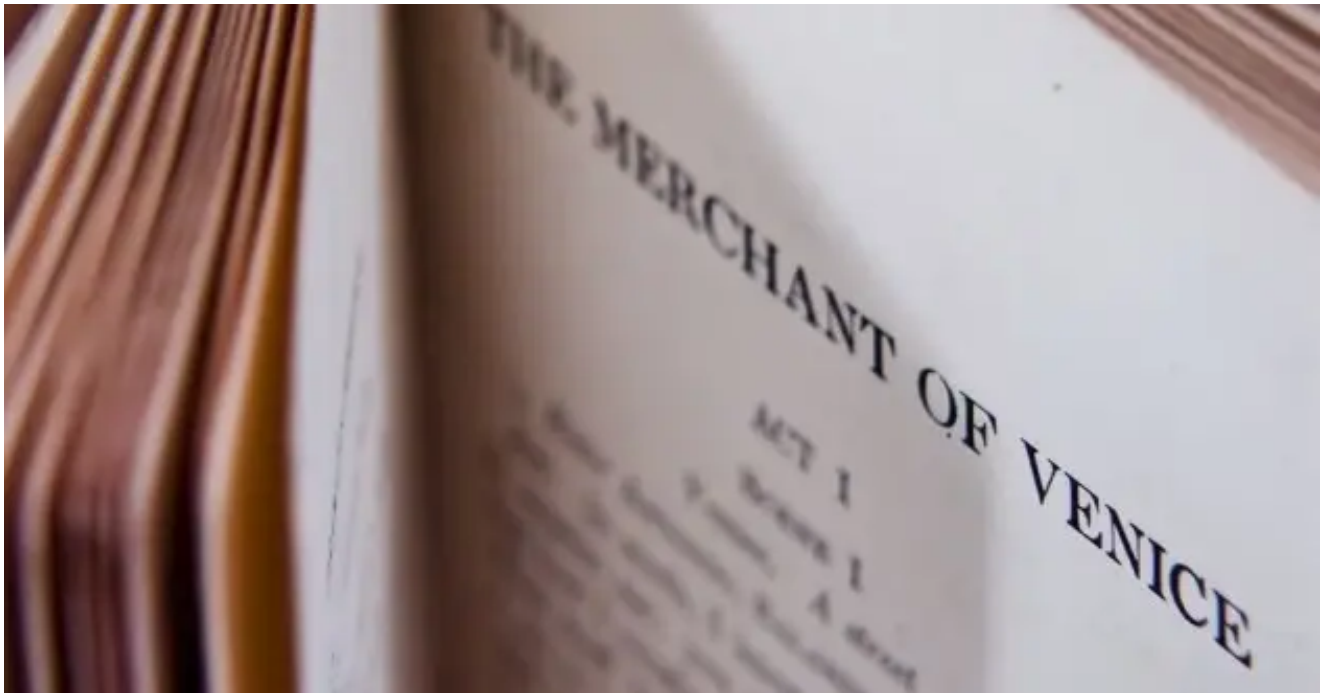
 [securityintelligence.com/merchant-of-fraud-returns-shylock-polymorphic-financial-malware-infections-on-the-rise/](http://securityintelligence.com/merchant-of-fraud-returns-shylock-polymorphic-financial-malware-infections-on-the-rise/)

February 15, 2012



[Home](#) &nbsp; [Banking & Finance](#)

Merchant of Fraud Returns: Shylock Polymorphic Financial Malware Infections on the Rise



Banking & Finance February 15, 2012

By [Amit Klein](#) 2 min read

Last September, we blogged about a new polymorphic financial malware variant we had discovered. We code-named it “Shylock” because every new build bundles random excerpts from William Shakespeare’s “The Merchant of Venice” in its binary. These are designed to change the malware’s file signature to avoid detection by antivirus programs and security software.

	<b>ucsvc.exe.742cfd2be5d44fa072802bd4b031e818.exe</b> File description: give me your blessing I am Launcelot your boy Company: And draw her home with music File version: 6.2.0.41 Date created: 31/08/2011 14:08 Size: 362 KB
	<b>fitMC.exe</b> File description: Shall witness I set forth as soon as you Company: That is done too sir only File version: 3.4.20.389 Date created: 04/09/2011 10:06 Size: 359 KB

In recent weeks, we have seen a significant increase in the number of end-user machines infected with Shylock. One of this malware’s distinguishing characteristics is its ability to almost completely avoid detection by antivirus scanners after installation. Shylock uses a unique three-step process to evade scanners:

## Step 1: Financial Malware Hides in Memory

---

Shylock injects itself into all running processes (applications) in memory. Every time a new application is initialized, Shylock suspends the application from running in memory, injects itself into the application process and then allows the application to proceed with its normal execution. Once installed, Shylock code doesn't run as a separate process; rather, it embeds itself within every genuine application running on a machine. This makes it very hard to detect. Moreover, even if Shylock is detected, the fact that it is embedded in multiple running applications makes it almost impossible to stop and remove from memory.

## Step 2: Watchdog Senses Scans

---

Shylock looks for and intercepts operations related to directory browsing and enumeration of registry keys, which indicate an antivirus scanning operation is underway. Once it detects "scanning" activity, Shylock deletes its own files and registry entries, making it undetectable. It remains active only in memory.

## Step 3: Hijacks Windows' Shutdown

---

Entries in the operating system registry allow malware (like any application or process) to execute its files as part of the start-up processes. Once Shylock has removed its files and registry entries to avoid being detected by an antivirus scan, it cannot survive a system shutdown/reboot. Any of these actions would remove it from memory and eliminate the infection. To ensure its survival, Shylock hooks into the Windows shutdown procedure and reinstates the files and registry keys (previously removed in Step 2) just before the system is completely shut down and after all applications are closed, including antivirus applications.

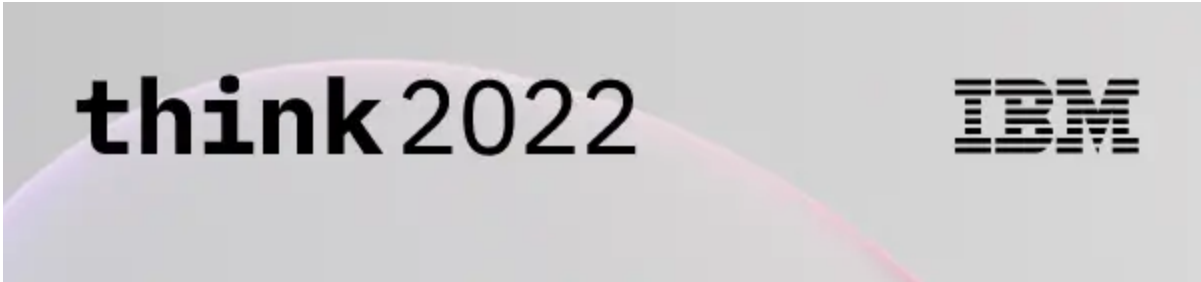
We have found that physically unplugging the machine's power source (assuming it does not have an internal battery) after Shylock has deleted its files and registry entries to evade detection will clean the memory and also the Shylock infection. Needless to say, we do not recommend this as a malware-removal practice.

[Antivirus](#) | [Financial Malware](#) | [Malware](#) | [Malware Injection](#) | [Operating System \(OS\)](#) | [Shylock](#) | [Threat Detection](#) | [Windows](#)

[Amit Klein](#)

CTO, Trusteer, an IBM company

As Trusteer's CTO, Amit Klein is responsible for researching and introducing game changing technologies into Trusteer's products, with particular focus o...

The image shows the IBM 'think 2022' logo. The word 'think' is in a lowercase, bold, sans-serif font, followed by '2022' in a larger, bold, sans-serif font. The background is a light gray with a subtle, abstract shape in shades of purple and pink.The image shows the classic IBM logo, consisting of the letters 'IBM' in a bold, sans-serif font, with horizontal stripes through the letters. The background is a light gray with a subtle, abstract shape in shades of purple and pink.

IBM Think Broadcast  
Let's think together.

Watch on demand →

