LizaMoon infection: a blow-by-blow account

By Fred Langa

A nasty piece of malware known as LizaMoon has hijacked links on millions of websites in the past weeks, including some normally safe iTunes and Google links.

Fortunately, LizaMoon is easy to avoid if you know what to look for.

Using rogue-AV scare tactics, LizaMoon tries to trick you into running bogus security-scan and virus-cleanup tools on your PC — but it's pure malware.

If allowed onto your PC, this particular ploy is especially troublesome because it can partially disable the Windows Security Center and change the Registry so that the full WSC can't be restarted. It also interferes with Microsoft Security Essentials, if MSE is running. (You'll find lots more LizaMoon news coverage via Google.)

My encounter with LizaMoon started unexpectedly one evening when a suspicious warning popped up on my screen. As discussed in a previous Top Story, I use Microsoft Security Essentials and the Windows 7 firewall to protect all of my PCs. In over a year of constant use, I'd never had any malware trouble. But that abruptly changed.

That evening, I was searching for something through Google — I don't recall what. When I clicked a link, a blank page overlaid with the dialog in Figure 1 popped up instead of the site I was expecting.

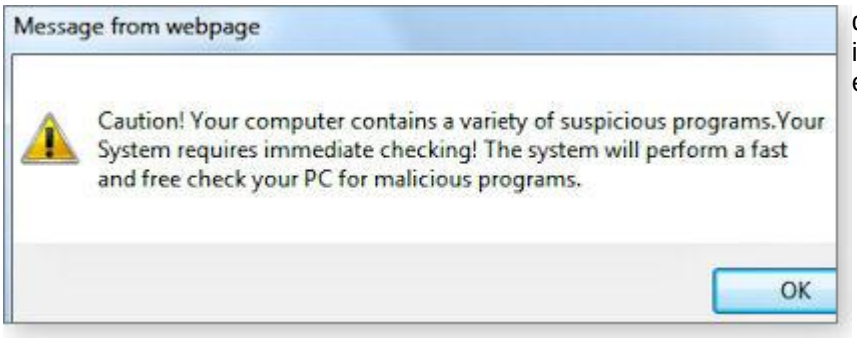

Figure 1. A real LizaMoon initial dialog, captured in the wild.

My mental alarm bells immediately started ringing — the dialog was identified as a **Message from webpage.** But why was a random, external webpage displaying what looked like a local security message?

Also, how could a random webpage know what was installed on my system (suspicious programs or not)? The warning made no sense.

There was plenty more to suggest that the dialog was bogus. For example, the third sentence is in fractured English — Microsoft dialogs aren't like that. And the kicker: I keep my system very clean, so the odds that it would suddenly contain "a variety of suspicious programs" are virtually nil.

Then it struck me. I'd encountered a for-real LizaMoon page hijack, in the wild!

Typically, when you encounter any suspicious webpage dialog, the correct procedure is to immediately dismiss it via the **red-X close box** in the upper-right corner of the dialog box or to simply close the browser. (If needed, you also can use Windows' Task Manager to kill offending software or its processes.)

Next, if you think you might have a security problem, you should manually launch known-good security

tools directly from reliable sources. In no case should you ***ever*** launch unknown software triggered by visits to random websites.

In my case, however, this was exactly the kind of malware I'd been looking for to test. In the past few months, readers reported encountering new malware that masquerades as a security tool — malware that disables or bypasses Microsoft Security Essentials. I'd been trying to track it down for weeks. And suddenly, there it was.

Living dangerously: taking the malware's bait

Given this unexpected opportunity, I took a deep breath and clicked OK, knowing full well that I was voluntarily giving the webpage permission to interact with my PC.

A new webpage opened, showed a flurry of fake "scanning" activity (most likely, just an animated **.gif**), and then reported a huge number of discovered viruses and security problems.

I knew my system was clean, so this report of widespread infection was clearly fake. But because the page layout and icons closely mimic those of familiar Windows tools, it could easily fool casual users into thinking that the alert was real.

After a minute of fake scanning activity, a new dialog opened — offering to "Remove all" the threats (see Figure 2).

Figure 2. Clicking "Remove all" on this fake security dialog starts the malware download. Find a way to close the dialog, as discussed in the text.

The new dialog set off more of my internal alarm bells. Windows normally identifies the software or subsystem involved in security alerts — such as the Action Center, the Security Center, Security Essentials, or whatnot. A dialog simply labeled "Windows Security Alert" is suspiciously generic.

And what's this about "Windows Defender"? That's Microsoft's standalone anti-malware tool that ships with Vista and Win7 and is available as a free download (page) for XP. The forerunner of the more

complete Microsoft Security Essentials, it's deactivated when you install MSE. Since I have MSE active on my system, I shouldn't be hearing from Windows Defender.

At that point, you'd normally try to dismiss the warning by clicking on the red X. To see what would happen next, I clicked "Remove all," knowing I was inviting trouble.

(If you're keeping count — and I did — you'll know this was my second entirely voluntary action leading to infection.)

A real and quite legitimate Windows file-download security warning opened, as shown in Figure 3. But while the previous dialog discussed "Windows Defender," this dialog box asked permission to download an installer for "Internet Defender." What's more, the dialog clearly showed that the file was from a site called update65.saceck.co.cc — not Microsoft!

Clearly, the LizaMoon authors are confident that people do not pay attention to these details.

Figure 3. This dialog box has several naming inconsistencies: the previous dialog mentioned Windows Defender, but this one offers something called Internet Defender. It also isn't coming from a known address, such as Microsoft.com.

Ignoring yet another opportunity to bail out before being infected, I clicked the Save button and entering the location where the file should be saved (the third voluntary action on the path to infection).

My hard-drive light flickered briefly and I swallowed hard, knowing that a malicious payload had just been delivered to my personal PC. (Yes, my system was fully backed up and my sensitive data encrypted.)

Ready or not, the malicious payload arrives

I intended to disconnect my PC from the network before the malware ran, assuming that going offline would keep any system damage local and no personal data could be exported.

But there must have been a script running somewhere, because the malware installer immediately attempted to self-start. Fortunately, Windows reported an **NSIS error** (see Figure 4). NSIS is SourceForge's Nullsoft Scriptable Install System, and the error means that an installation script failed an integrity check.

Figure 4. The first sign of trouble after downloading the malware

Following the link given with the NSIS Error opens a sourceforge.net page advising you to "Update your anti-virus software" and to "Scan for, and remove malware and viruses on your system."

Microsoft.com's "NSIS Error" page states that, among other possible causes, "Your PC is infected with a virus." It adds, "Thoroughly scan your PC for possible virus or spyware infections." The page even provides a direct link to Microsoft's free online safety scanner (site) and to a discussion of how to remove viruses and malware.

I took none of that advice but did disconnect from the network. Taking yet another deep breath (and my fourth voluntary action), I clicked OK, which let the malware installer run to completion.

The malware goes active and disables my security

Immediately after I clicked OK, my system went haywire.

First, the Windows Security Center was compromised (see Figure 5), and I could not manually relaunch it

— proof that my system was infected.

Figure 5. The infection immediately disabled the Windows Security Center.

Next, the downloaded malware opened a new, fake, scanning window. Calling itself "System Defender," it claimed to have discovered numerous malware apps. Trying to learn what I could about the bogus software, I opened its Help/About menu, as shown in Figure 6.

Figure 6. Superficially, this dialog looks quite legit. But it fails closer inspection — it can't even keep its name straight!

In previous dialog boxes, the malware identified itself as "Windows Security" and "Windows Defender." Now it's simultaneously "System Defender" and "Internet Defender." No valid software product goes by four separate names in the same instance.

Of course, the point of all this smoke-and-mirrors chicanery is confusion — to extort you into ***paying*** to activate the software and "remove" the supposed infections. But the only real infection is LizaMoon itself.

I was certain that clicking the malware's Remove All button would bring me to a payment site. But because I didn't want to reconnect to the Net while the malware was still active on my machine, I left the above dialog alone and waited to see what would happen.

Every few minutes, the malware would pop up other warnings, such as the one in Figure 7. There were many others.

Figure 7. The fake virus warning got more urgent — and more illogical and ungrammatical. This nonsensical message states that a firewall has somehow detected keylogging in a social network.

Throughout this time, Microsoft Security Essentials was silent — a major disappointment. However, every few minutes the Windows Security Center would wave the flag (via a dialog box) and urge me to "Turn on Windows Security Center service (Important)."

LizaMoon blocked attempts to restart the Security Center service and hid itself from MSE. To clean up the mess, I needed to use another tool, Malwarebytes Anti-Malware (site/download), which disabled and removed most of the malware (Figure 8). When I rebooted the newly cleaned PC, I ran MSE again, which discovered more pieces (Figure 9).

Figure 8. Malwarebytes' Anti-Malware disabled and removed most — but not all — of the malware.

Figure 9. MSE was able to remove the threats that Malwarebytes missed.

I followed up with scans using ESET's online scanner, McAfee's Security Scan Plus, TrendMicro's HouseCall, and Microsoft Windows Live OneCare scanner. All agreed that my PC was now clean.

Just in case, I continued to run additional extra scans for the next few days. Nothing untoward turned up, and my system has behaved normally ever since.

Microsoft Security Essentials: first failure

I have to say I'm disappointed that Microsoft Security Essentials didn't detect or prevent this infection. It should have, and I hope Microsoft patches MSE pronto.

On the other hand, deliberate choices and actions by a user can defeat ***any*** software. LizaMoon required my active, voluntary involvement ***four different times*** before the infection took hold.

LizaMoon wasn't even subtle: I had plenty of warnings and opportunities to abort the process, the malware itself provided abundant clues to its own bogus nature (such as an inability to keep its aliases straight).

The lesson? Using security tools is no substitute for common sense. Malware like this is actually very easy to avoid, ***if*** you pay attention to what's going up on your screen.

Thoroughly read all dialogs — especially unexpected ones and ones pertaining to installing new software. Ask yourself if the warning really make sense. If you have any suspicions at all, dismiss such dialogs via the red-X close box or, if that fails, by using the aforementioned built-in Task Manager (more info).

Immediately run your favorite suite of security tools, such as the ones mentioned above.

Remember: You won't get infected with LizaMoon (and similar malware) unless you allow it!