Some Linux Mint downloads on February 20 not at all sweet

23 February 2016, by Nancy Owano

What a way to end a weekend. Those who know a thing or three about systems in general and Linux fans may have felt his pain. The Linux Mint Blog carried a post after midnight Saturday in the wee hours of Sunday from the creator of Mint, Clem Lefebvre.

"I'm sorry I have to come with bad news. We were exposed to an intrusion today. It was brief and it shouldn't impact many people, but if it impacts you, it's very important you read the information below. What happened? Hackers made a modified Linux Mint ISO, with a backdoor in it, and managed to hack our website to point to it. Does this affect you? As far as we know, the only compromised edition was Linux Mint 17.3 Cinnamon edition."

Anyone downloading another release or edition was not affected, he said. Likewise, anyone who downloaded via torrents or direct HTTP link was not affected. Thirdly, he wrote in the blog, it should only impact people who downloaded this edition on Saturday, February 20.

In brief then the breach affected those who downloaded Linux Mint 17.3 Cinnamon edition on Saturday, 20 February.

Steven J. Vaughan-Nichols walked *ZDNet* readers through what would have happened to victims. "The result was that when a user tried to download 64-bit version of the Linux Mint 17.3 with the Cinnamon desktop, the most popular edition, they were directed to a rogue download server. Once there, a user would be sent a hacked copy of Mint containing the Tsunami malware program. This backdoor enables the controller to remotely access the system."

The good news, said *ZDNet*, was that users of Linux Mint spotted the problem early. Lefebvre took down the site to prevent the polluted Mint ISO images from being distributed any further.

His recommendations for what to do if affected included deleting the ISO and if anyone burnt it to DVD, to trash the disc. If burnt to USB, format the stick. If ISO was installed on a computer, he said to put the computer offline, back up personal data, reinstall the OS or format the partition and change passwords for sensitive websites, particularly email.

On the 1:44 am Sunday post he had said everything was not yet back to normal. He said they took the server down while "we're fixing the issue."

They traced the incident source back to Bulgaria, but they did not know what the motive could be. The breach was made via wordpress. From there they got a www-data shell.

In his exchange with reader responses, Lefebvre said the intrusion was from a 64-bit version and that it looked as if the intruders had been preparing to compromise the 32-bit as well later on.

Then in a subsequent blog post timed 3.05 pm on Sunday, it became clear that more than just the distro version was affected. He wrote that all forums users should change their passwords.

"It was confirmed that the forums database was compromised during the attack led against us yesterday and that the attackers acquired a copy of it. If you have an account on forums.linuxmint.com, please change your password on all sensitive websites as soon as possible. The database contains the following sensitive information: Your forums username; an encrypted copy of your forums password;your email address; any personal information you might have put in your signature/profile/etc…; any personal information you might written on the forums (including private topics and private messages)."

Back in 2013, David Hayward, writing in *TechRadar*, explored reasons behind Mint's rise in popularity.

"Mint has become the very best example of what a Linux desktop should be: fast, easy, pleasing to the eye, useful and productive. Others, still, see Mint as the ideal desktop for Windows refugees, or those who are trying out Linux for the first time, and want an operating system that essentially works 'out of the box', playing any number of media files from a variety of sources. Whatever the reason, we can be sure that Linux Mint has evolved into something more than just another Linux distribution, and that its popularity has fueled its own style and usefulness."

Heavy sits the crown. Is that the price an operating system, even Linux, has to pay for being popular?

An interesting message to Lefebvre on the Linux Mint site on Monday: "To the Mint team: take it as a compliment. As the saying goes, the higher you get, the more of a target you become. Also, when you handle problems well like you are now, it actually ends up benefiting you in the end. Your users will trust you even more than they already do."

Threatpost said that according to DistroWatch.com, which tracks Linux distributions by number of page hits over a given period of time, "Mint is far and away the most popular build, surpassing Debian, Ubuntu, and Fedora."

At times elsewhere we hear about break-ins and thefts elsewhere, where the affected tech leadership fails to rush out information to share messy details for what was stolen and when they do, issue terse statements that they are concerned and are looking into the matter. Assessing the events, Chris Brook of *Threatpost* made note of Lefebvre's transparency.

Lefebvre straight out shared the news and went into detail on the blog as to who might be affected and what to do.

"Lefebvre has been transparent about the breach since it was announced, further clarifying that attackers managed to breach Linux Mint's site in the first place via a WordPress vulnerability and from there they got a www-data shell. They were running the latest build of WordPress but a custom theme and 'lax file permissions for a few hours' led to the hack," he wrote.

In fact, researchers at Kaspersky Lab had a look at some of the compromised ISO images. What was this malware all about? They saw that the malware was "a simple backdoor that's controlled through an unencrypted IRC connection. It's capable of a few things: Running types of UDP and TCP flooding for DDoS attacks, downloading arbitrary files to the machine, and executing arbitrary commands," wrote Brook.

More information: blog.linuxmint.com/?p=2994